T.C.
DÜZCE ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

KURUMSAL AĞLARIN SİSTEMATİK TASARIMI İÇİN YENİ BİR DİNAMİK VLAN YAKLAŞIMI

SERDAR KIRIŞOĞLU

DOKTORA TEZİ
ELEKTRİK-ELEKTRONİK VE BİLGİSAYAR MÜHENDİSLİĞİ
ANABİLİM DALI

DANIŞMAN
PROF. DR. RESUL KARA

DÜZCE, 2018

T.C.
DÜZCE ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

KURUMSAL AĞLARIN SİSTEMATİK TASARIMI İÇİN YENİ BİR DİNAMİK VLAN YAKLAŞIMI

Serdar KIRIŞOĞLU tarafından hazırlanan tez çalışması aşağıdaki jüri tarafından Düzce Üniversitesi Fen Bilimleri Enstitüsü Elektrik-Elektronik ve Bilgisayar Mühendisliği Anabilim Dalı'nda **DOKTORA TEZİ** olarak kabul edilmiştir.

Tez Danışmanı

Prof. Dr. Resul KARA

Düzce Üniversitesi

Jüri Üyeleri

Prof. Dr. Resul KARA
Düzce Üniversitesi _____

Doç. Dr. Pakize ERDOĞMUŞ
Düzce Üniversitesi _____

Doç. Dr. İbrahim ÖZÇELİK
Sakarya Üniversitesi _____

Dr. Öğr. Üyesi Murat İSKEFİYELİ
Sakarya Üniversitesi _____

Dr. Öğr. Üyesi Fatih KAYAALP
Düzce Üniversitesi _____

Tez Savunma Tarihi: 01/08/2018

BEYAN

Bu tez çalışmasının kendi çalışmam olduğunu, tezin planlanmasından yazımına kadar bütün aşamalarda etik dışı davranışımın olmadığını, bu tezdeki bütün bilgileri akademik ve etik kurallar içinde elde ettiğimi, bu tez çalışmasıyla elde edilmeyen bütün bilgi ve yorumlara kaynak gösterdiğimi ve bu kaynakları da kaynaklar listesine aldığımı, yine bu tezin çalışılması ve yazımı sırasında patent ve telif haklarını ihlal edici bir davranışımın olmadığını beyan ederim.

01 Ağustos 2018

Serdar KIRIŞOĞLU

TEŞEKKÜR

Doktora öğrenimimde ve bu tezin hazırlanmasında gösterdiği her türlü destek ve yardımdan dolayı çok değerli hocam Prof. Dr. Resul KARA'ya en içten dileklerimle teşekkür ederim.

Bu çalışma boyunca yardımlarını ve desteklerini esirgemeyen sevgili eşim, annem, babam ve aileme sonsuz teşekkürlerimi sunarım.

Bu çalışmayı sevgili eşim, hayat arkadaşım, çocuklarımın annesi, Tuba KIRIŞOĞLU'na ithaf ediyorum.

01 Ağustos 2018 **Serdar KIRIŞOĞLU**

İÇİNDEKİLER

Sayfa No

ŞEKİL LİSTESİ VII

ÇİZELGE LİSTESİ VIII

KISALTMALAR IX

ÖZET X

ABSTRACT XI

EXTENDED ABSTRACT XII

1. GİRİŞ 1

1.1. KURUMSAL AĞLARIN TASARIMI 2

1.1.1. Klasik Ağ Tasarımı 2

1.1.2. Sistematik Ağ Tasarımı 3

1.2. VLAN 3

1.3. VLAN TÜRLERİ 5

1.4. STATİK VE DİNAMİK VLAN 5

1.5. İLGİLİ ÇALIŞMALAR 6

2. BASİT AĞ YÖNETİM PROTOKOLÜ 12

2.1. SNMP'NİN GELİŞİMİ 13

2.2. SNMP'NİN MİMARİ YAPISI 14

2.2.1. Ajan Uygulama 15

2.2.2. Yönetici Uygulama 16

2.2.3. Ağ Yönetim Sistemi 16

2.3. SNMP İLETİŞİMİ 16

2.3.1. SNMP Paket Sırası 16

2.3.2. SNMP Paket Yapısı 18

2.3.3. MIB ve OID Kavramları 22

2.4. SNMP VE C# 24

2.5. ANAHTARLARDA SNMP KONFIGÜRASYONU 24

3. SNMP İLE DİNAMİK VLAN MODELLEMESİ 26

3.1. MATEMATİKSEL MODELİ VE EŞİTLİKLERİ 26
3.2. ALGORİTMA VE AKIŞ DIYAGRAMLARI 29
4. SNMP'YE DAYALI DİNAMİK AĞ TRAFİĞİ DENGELEME ALGORİTMASI PERFORMANS DEĞERLENDİRMESİ 35
4.1. PERFORMANS DEĞERLENDİRME ORTAMI 35
4.2. ALGORİTMA ÇALIŞMA SÜRESİ 38
4.3. UYGULANAN SENARYOLAR 38
4.4. KURUMSAL AĞ SİSTEMATİK YAKLAŞIMLARI İLE KARŞILAŞTIRMA 52
4.4.1. VLAN Başına Düğüm Sayısı Kriterine Göre Karşılaştırma 54
4.4.2. Broadcast Trafik Kriterine Göre Karşılaştırma 56
4.5. BENZER ÇALIŞMALARA KARŞI AVANTAJ VE DEZAVANTAJLARI 57
5. SONUÇLAR VE ÖNERİLER 59
5.1. SONUÇLAR 59
5.2. ÖNERİLER 62
5.3. ÇALIŞMANIN GETİRDİĞİ KATKILAR 62
6. KAYNAKLAR 64
ÖZGEÇMİŞ 68

ŞEKİL LİSTESİ

Sayfa No

Şekil 1.1. Vmware dağıtık anahtar yapısı görünümü 7
Şekil 2.1. SNMP mimarisi 15
Şekil 2.2. SNMP paket sırası 17
Şekil 2.3. SNMP paket yapısı 18
Şekil 2.4. SNMP paket içeriği 18
Şekil 2.5. SNMPv1 PDU çeşitleri 20
Şekil 2.6. SNMPv2 PDU çeşitleri 21
Şekil 2.7. SNMPv3 PDU mesaj yapısı 21
Şekil 2.8. MIB ağaç yapısı OID numaraları. 23
Şekil 3.1. SNMP'ye dayalı dinamik VLAN ekleme algoritması akış diyagramı. 30
Şekil 3.2. SNMP'ye dayalı dinamik VLAN yük dengeleme algoritması akış diyagramı. 31
Şekil 3.3. Ağa dahil olan düğümler için üyelik akış diyagramı. 32
Şekil 3.4. SNMP'ye dayalı dinamik VLAN ekleme algoritması. 33
Şekil 3.5. SNMP'ye dayalı dinamik VLAN yük dengeleme algoritması. 33
Şekil 4.1. Başlangıç ve reset durumu VLAN üyelikleri. 39
Şekil 4.2. Güvenli VLAN senaryosu topolojisi. 41
Şekil 4.3. Ağa düğüm eklenmesi durumu. 42
Şekil 4.4. Senaryo 4 başlangıç düğümlerinin VLAN'lara dağılımı. 43
Şekil 4.5. Senaryo 4 tüm düğümlerin oluşturduğu trafiğin VLAN'lara dağılımı. 44
Şekil 4.6. VLAN eşik değeri değişimi sonucu VLAN trafik dağılımları. 45
Şekil 4.7. VLAN'lar için eşik değerinin belirlenebileceği yazılım arayüzü. 45
Şekil 4.8. Özel güvenlik düzeyine sahip düğümün yer değiştirmesi. 47
Şekil 4.9. Normal düğüm ağda yer değiştirmesi. 48
Şekil 4.10. Ağdaki düğüm sayısının arttırılması. 49
Şekil 4.11. Ağdaki düğüm sayısının arttırılması. 51
Şekil 4.12. VLAN başına düşen düğüm grafiksel gösterimi 55
Şekil 4.13. VLAN başına Broadcast trafiği 56

ÇİZELGE LİSTESİ

Sayfa No

Çizelge 2.1. SNMP avantaj ve dezavantajları 12
Çizelge 2.2. SNMP OSI ve TCP/IP. 13
Çizelge 2.3. SNMP versiyonları ve karşılaştırması 14
Çizelge 2.4. SNMP paketi boyut ve içeriği 19
Çizelge 2.5. SNMPv3 mesaj başlık alanları 21
Çizelge 2.6. SNMP için kullanılan hazır kütüphaneler 24
Çizelge 4.1. Başlangıç ve reset durumu VLAN üyelikleri 39
Çizelge 4.2. Senaryo 2'de algoritma sonucu VLAN üyelikleri. 40
Çizelge 4.3. Düğümler tarafından üretilen trafik değerleri. 42
Çizelge 4.4. Ağa sonradan dahil olan düğümler ve trafikleri. 43
Çizelge 4.5. Senaryo 5, VLAN ekleme algoritması için düğüm trafikleri. 44
Çizelge 4.6. Özel güvenlik düzeyi konum değişimi. 47
Çizelge 4.7. Düğümlerin fiziksel olarak konum değiştirilmesi. 48
Çizelge 4.8. Ağdaki düğüm sayısının 36'ya çıkarılması. 50
Çizelge 4.9. Düğüm sayısısın maksimum yapılması. 51
Çizelge 4.10. Toplam trafiğin arttırılması. 52
Çizelge 4.11. Karşılaştırma için kullanılan ağ parametreleri. 53
Çizelge 4.12. VLAN başına düşen düğüm sayısı. 55
Çizelge 4.13. Tahmini Broadcast trafiği değerleri 56
Çizelge 4.14. Çalışmanın kriterlere göre diğer çalışmalar ile karşılaştırılması. 58

KISALTMALAR

ACL	Access Control List
DHCP	Dynamic Host Configuration Protocol
DOD	Department Of Defense
HTTP	Hyper-Text Transfer Protocol
IEEE	The Institute of Electrical and Electronics Engineers
IP	Internet Protocol Address
ISO	International Standart Organization
LAG	Link Aggregation Group
LAN	Local Area Network
MAC	Media Access Control
MIB	Management Information Base
MGMT	Network Management Entries
NMS	Network Management System
OID	Object Identifier
OSI	Open Systems Interconnection
PDU	Protocol Data Unit
RADIUS	Remote Authentication Dial-in User Service
SDN	Software Defined Network
SNMP	Simple Network Management Protocol
SSH	Secure Shell
STP	Spanning Tree Protocol
TCP	Transmission Control Protocol
VDS	vSphere Distributed Switch
VLAN	Virtual Local Area Network
VMPS	VLAN Management Policy Server
VPN	Virtual Private Network
VTP	VLAN Trunking Protocol
WAN	Wide Area Network

ÖZET

KURUMSAL AĞLARIN SİSTEMATİK TASARIMI İÇİN YENİ BİR DİNAMİK VLAN YAKLAŞIMI

Serdar KIRIŞOĞLU
Düzce Üniversitesi
Fen Bilimleri Enstitüsü, Elektrik-Elektronik ve Bilgisayar Mühendisliği Anabilim Dalı
Doktora Tezi
Danışman: Prof. Dr. Resul KARA
Ağustos 2018, 67 Sayfa

Günümüzde kurumsal ağların büyüklüğü ve karmaşıklığı oldukça artmıştır. Kurumsal ağların tasarımları, ağın sahibi olan büyük ölçekli firmalar, üniversiteler, devlet kurumları veya diğer büyük organizasyonlar tarafından yapılmaktadır. Ağın performansı artırmak, güvenlik yönetimini kolaylaştırmak ve adres yönetimini sağlamak için kurumsal ağların tasarımında sıklıkla Sanal Yerel Alan Ağları (VLAN-Virtual Local Area Network) kullanılır. Bu çalışmada, kurumsal ağlarda bulunan VLAN'larda dengeli ağ trafiği taşınmasını sağlayan yeni bir sistematik yaklaşım sunulmaktadır. Bu yaklaşım için önerilen metot, aynı güvenlik düzeyine sahip VLAN'lardaki toplam trafiğe göre, düğümlerin VLAN üyeliklerini dinamik olarak değiştirmektedir. Özel güvenlik düzeyine sahip olan VLAN'lara üye olması gereken düğümler için ağın her noktasından aynı VLAN'a üye olması bu yaklaşımın getirdiği esnekliklerden biridir. Bu metoda göre ağda bulunması gereken VLAN sayısı, parametrik veya sabit öndeğerli olarak ayarlanabilmekte, her bir VLAN'da trafik oluşturan üyelerin, yaklaşık eşit şekilde dağıtılması sağlanmaktadır. Bu sayede VLAN'da eşit ya da birbirine yakın trafik değerleri oluşmaktadır. Bu metodun işlevselliğini test etmek için Basit Ağ Yönetim Protokolü (SNMP- Simple Network Protocol) temelli bir yazılım geliştirilmiş ve gerçek ağ ortamında uygulanarak önerilen amaçlara ulaşılmıştır. Ağdaki VLAN başına düşen düğüm sayısı ve VLAN broadcast trafiği açısından literatürde yer alan kurumsal ağlar için sistematik ağ yaklaşımı içeren çalışmalarla karşılaştırılmıştır.

Anahtar sözcükler: Kurumsal ağ, Sanal yerel alan ağları, Sistematik ağ yaklaşımı, SNMP, Trafik yük dengelemesi.

ABSTRACT

A NEW DYNAMIC VLAN APPROACH FOR SYSTEMATIC DESIGN OF ENTERPRISE NETWORKS

Serdar KIRIŞOĞLU
Düzce University
Graduate School of Natural and Applied Sciences, Department of Electric-Electronic and Computer Engineering
Doctoral Thesis
Supervisor: Prof. Dr. Resul KARA
August 2018, 67 Pages

Nowadays, the size and complexity of corporate networks has increased considerably. The designs of enterprise networks are made by large-scale companies, universities, government agencies or other large organizations that own the network. Virtual local area networks (VLAN) are often used in the design of enterprise networks to improve network performance, facilitate security management, and provide address management. This work presents a new systematic approach to network traffic that is balanced across VLAN's in corporate networks. The recommended method for this approach is to dynamically change the VLAN membership of the nodes according to the total traffic in the VLANs with the same security level. One of the flexibility of this approach is that VLANs with a specific level of security must be members of the same VLAN for every node in the network that needs to be a member. According to this method, the number of VLANs that should be in the network can be set as parametric or constant prefix, and it is ensured that the members who create traffic in each VLAN are distributed approximately evenly. In this way, equal or near traffic values are generated in VLAN. In order to test the functionality of this method, a simple network management protocol (SNMP) based software has been developed and implemented in the real network environment to achieve the recommended objectives. The number of nodes per VLAN in the network and the VLAN broadcast traffic have been compared with studies involving a systematic network approach for corporate networks in the literature.

Keywords: Enterprise network, Network traffic load balancing, Systematic approach network, SNMP, Virtual local area networks.

EXTENDED ABSTRACT

A NEW DYNAMIC VLAN APPROACH FOR SYSTEMATIC DESIGN OF ENTERPRISE NETWORKS

Serdar KIRIŞOĞLU
Düzce University
Graduate School of Natural and Applied Sciences, Department of Electric-Electronic and Computer Engineering
Doctoral Thesis
Supervisor: Prof. Dr. Resul KARA
August 2018, 67 Pages

1. INTRODUCTION

In this study, an algorithm was developed to adjust the total traffic of each virtual network to be close to each other for use in virtual local area networks. While the total traffic of the virtual local area network is being calculated, the total traffic generated by the nodes belonging to the virtual network is considered. In each algorithm cycle, the memberships of the nodes have been tried to reach the target by changing if necessary.

2. MATERIAL AND METHODS

A software for the implementation of this algorithm has been developed and used in a real-time network. The software that uses this algorithm is communicated with the end devices on the network using the SNMP protocol. A DHCP server was set up for IP reception according to the virtual local network to which the nodes belong. A database is used to store information about nodes and end devices. In the environment, virtual local networks use a backbone key to communicate with each other when needed. In addition, different VLANs have been created according to the security levels of each node. According to the level of security, the necessary node information is recorded in the database.

3. RESULTS AND DISCUSSIONS

As a result, each virtual local area network, in each cycle of the algorithm, has close traffic values. Nodes with different security levels are not able to access resources other than their rights. Nodes that do not have different levels of security have been observed to

change VLAN memberships whenever needed, in each cycle of the algorithm.

4. CONCLUSION AND OUTLOOK

As a result the work has reached its goal. VLANs dynamically contain different nodes. And each has reached a level of traffic close to each other. There are advantages and disadvantages to the literature in comparison with other similar works. These advantages and disadvantages are detailed in the thesis. It is aimed that this thesis study will be developed in the future with the use of more up-to-date technology in line with the same targets.

1. GİRİŞ

Bu bölümde kurumsal ağlar, kurumsal ağların tasarımı, VLAN, VLAN türleri, Dinamik ve Statik VLAN kavramlarına değinilmiş ve literatürde yer alan bu çalışmaya benzer diğer çalışmalar özetlenmiştir.

Günümüzde bilgisayar ağları Geniş Alan Ağları (WAN-Wide Area Network), LAN ve alt kümesi olan VLAN olarak üç ana başlık altında toplanabilir. WAN uzak lokasyonların birbirleri ile iletişim sağlaması için, LAN ise aynı lokasyonda ve arada bir yönlendirici bulunmadan çalışabilecek şekilde tasarlanmıştır. VLAN ise, sayısı gittikçe artan ağdaki uç cihazların internet erişimini ve birbirleri ile olan iletişimini daha kolay organize edebilmeleri ve yönetilebilmeleri için kullanılmaktadır. VLAN adından da anlaşılacağı üzere gerçek bir LAN'ı alt ağlara ayırıp daha kolay izlemek ve yönetmek için sanal olarak alt ağlara ayırmak için kullanılır.

Kurumsal ağlar ise belirli bir kurumun lokasyon gözetmeksizin bütün kullanıcı ve ağ cihazlarının sanki aynı LAN'daymış gibi birbirleriyle hızlı ve güvenli bir iletişim kurmaları için tasarlanmış, içinde farklı teknolojiler ve ağ cihazları barındırabilen ağlara denmektedir. Örneğin bir üniversite tek bir kampüsten oluşmayabilir. Uzak bir konumda bir bölüme sahip olabilir. Ancak bu konum için kampüsten ayrı bir LAN kurulabileceği gibi kampüs içindeki LAN'a da dahil olabileceği teknolojiler mevcuttur. Bu iki konumu birbirine bağlayabilen ve tek bir LAN tasarımı oluşturulabilecek teknolojiye Sanal Özel Ağ (VPN-Virtual Private Network) denmektedir. Kurumsal ağlara birçok örnek verilebilir, fabrikalar da bunlardan biridir. Masaüstü bir uygulama merkez fabrikadan, üretim yapılan ayrı bir uzak konumdaki bir cihaza ya da bir otomasyona bağlanma gereği duyabilir. Bunun çözümü de yine aynı şekilde VPN kullanmak olacaktır. Kurumsal ağların, büyüyerek karmaşıklığı arttıkça ve kurumsal gereksinimlere ihtiyaç duydukça tasarımlarını değiştirmek gerekmektedir. Bu durum ağ yöneticilerinin karşılaştığı en önemli problemlerden biridir [1]. Bundan dolayı kurumsal ağlarda ister tek bir konum ister uzak konumlar da dahil olsun VLAN teknolojisinin kullanımı ağ yöneticilerinin işini yönetilebilirlik esneklik ve güvenlik açısından kolaylaştırmaktadır.

Ağ üzerinden transfer edilen veri miktarının artması, uç kullanıcı sayısının artması ve

teknolojinin getirdiği yeni ağ servislerinin bant genişliği ihtiyacının artmasına rağmen veri iletim yollarındaki teknolojik gelişmenin aynı oranda ilerlememesi ile bazı sıkıntılarla karşılaşılmaktadır. Bu tez çalışmasında kurumsal ağlarda geleneksel ağ yönetiminin sayılan sebeplerle zorlaşması nedeniyle, istemcilerin kullandıkları bant genişliği için yük dengelemesinin, dinamik VLAN üzerinde uygulanmasına olanak sağlayan, VLAN bazlı trafik yük dengelemesi kelimelerinin baş harflerinden oluşan *VLAN_BTYD* adında bir algoritma geliştirilmiş ve buna dayalı bir sistematik yaklaşım sunulmuştur. Bu bölümün birinci kısmında kurumsal ağların tasarımı, ikinci kısmında VLAN kavramı, üçüncü kısmında algoritmanın alt yapısında kullanılacak olan SNMP protokolü ve dördüncü kısmında literatürdeki benzer çalışmalara değinilmiştir.

1.1. KURUMSAL AĞLARIN TASARIMI

Son zamanlardaki deneysel çalışmalar kurumsal ağların büyüklüğü ve yönlendirme dizaynlarındaki karmaşıklıklarının, taşıyıcı ağlarına rakip olduğunu veya aştığını göstermektedir [2], [3].

Günümüzde taşıyıcı ağlardan çok daha fazla kurumsal ağ kullanılmaktadır ve tasarımları bireysel şirketlerin, üniversitelerin, devlet kurumlarının veya diğer türdeki organizasyonların ihtiyaçlarına göre özelleştirilmektedir. Bununla birlikte, karmaşıklık, yaygınlık ve çeşitliliğe rağmen, kurumsal ağlar araştırmacılar tarafından çok az ilgi görmüştür [4].

Kurumsal ağ yöneticileri benzersiz tasarım zorlukları ile karşı karşıyadırlar. Taşıyıcı ağ yöneticilerinden daha geniş bir güvenlik, esneklik ve performans gereksinimlerini karşılamaları gerekmektedir. Örnek olarak, farklı kullanıcı gruplarının yönetimini kolaylaştırmak için VLAN yapılandırılması [5], şirket birleşmelerini desteklemek için çoklu yönlendirme alanlarının entegrasyonu [3] ve giriş filtrelemesi yapmak ve ayrıcalıklı veritabanlarına erişimi kontrol etmek için paket filtrelerin kurulumu verilebilir [6].

1.1.1. Klasik Ağ Tasarımı

Kurumsal ağların klasik tasarım yaklaşımıyla yönetilmesi esnasında birçok zorluklarla karşılaşılmaktadır. Öncelikle ağ yöneticisi fiziksel olarak doğru tasarım yapmalıdır. Bu yaklaşımda, ağda bir yönetici ağ cihazlarını ya merkezi bir yönetim sunucusundan ya da fiziksel olarak cihazın yanına giderek yapılandırmak zorundadır. Ayrıca düğümleri ya

çalışma gruplarına ya da güvenlik düzeylerine göre gruplandırmalıdır.

Ağ yöneticisi bunları yaparken aynı zamanda ağın trafik yoğunluğunu dinlemeli ve buna göre ya ağa yeni bir VLAN eklemeli ve üyelikleri tekrar düzenlemeli ya da mevcut VLAN'lar ile bir çözüm sunmaya çalışmalıdır. Öte yandan, ağ yöneticisi performans, yönetilebilirlik kolaylığı, güvenlik ve başarısızlıklara karşı direnç gibi üst düzey kısıtlarla karşı karşıyadır [4]. Öte yandan, bir ağ tasarımını gerçekleştirebilmek için, bir yöneticinin bir dizi protokolden, düşük seviyeli mekanizmalardan ve seçeneklerden elle seçimler yapması gerekmektedir. Bu protokollerin ve mekanizmaların çoğu derin etkileşimlere sahiptir. Bununla birlikte, ağ yapılandırmasının mevcut "protocol by protocol" yöntemi, ağ operatörünün bu etkileşimleri sistematik bir şekilde görmesini ve kontrol etmesini sağlamaz. Tasarım hataları ve konfigürasyon hataları, önemli sayıda ağ sorununa neden olmaktadır [7] ve son istatistiklere göre siber saldırıların %65'inden fazlası tarafından kullanılmaktadır [8].

1.1.2. Sistematik Ağ Tasarımı

Belirli kısıtlar çerçevesinde ağın fiziksel yapısı ve güvenliği ile alakalı önerileri, bir formülasyon sonucu; ağ yöneticisine, ağın tasarımının nasıl yapılacağına dair tavsiyeler vermek olan yaklaşıma Sistematik Ağ Tasarımı denir.

Bu tasarım yaklaşımında, ağdaki cihazlar, düğümler, Access Control List'ler (ACL), kullanıcı grupları, ve bant genişliğini etkileyecek her türlü faktör (Broadcast domain, düğümlerin trafikleri vb.), belirli bir formülasyona dökülür. Bu formülasyonun sonucuna göre ağ yöneticisine ağın tasarımında tavsiye niteliğinde yardımcı olunur. Bu yaklaşımda ağ yöneticisi kriterleri belirleyerek düğümlerin VLAN üyelikleri, ağda kaç adet VLAN olması gerektiği gibi önerileri formülasyondan çıkarım yaparak kısa sürede karar verebilir. Bu yaklaşım aslında ağ yöneticisinin belirlediği kısıtlara göre bir nevi optimizasyon çalışmasıdır.

1.2. VLAN

VLAN IEEE (802.3ac) tarafından geliştirilmiş ve LAN'larda, ağ kullanıcılarını ve kaynaklarını mantıksal olarak gruplandırarak Open Systems Interconnection (OSI) modelinde 2. katman trafiğinin, farklı VLAN'da yer alan anahtar arayüzleri arasında veri akışının engellenmesini sağlayan bir standarttır [9].

LAN'ları VLAN'lara ayırmak kontrol, performans, güvenlik ve ölçeklenebilirlik açısından hem ağ kullanımına hem de ağ kullanıcılarına yansıyacak olan avantajlar sağlamaktadır. VLAN kullanımının avantajları şöyle sıralanabilir;

a) Kontrol ve performans: LAN'da yayın paketleri tüm uç cihazlara kadar iletilirler. Bu durum gereksiz paket gönderimlerine yol açacağından bant genişliğini azaltmaktadır. VLAN kullanılarak bu durum kontrol altına alınabilir ve gereksiz yayın trafiğine engel olunur. Bir LAN'ı her bir birim için VLAN'lara ayırmak çok daha iyidir. VLAN'lar LAN'ı yayın bölgelerine (broadcast domain) ayırarak yayın trafiğini azaltır ve ağ performansının artırılmasını sağlar [10].

b) Güvenlik: LAN'da uç kullanıcılar birbirleriyle haberleşebilir, basit uygulamalar ile ağı dinleyebilir ve saldırı yapabilirler. LAN'ın VLAN'lara bölünmesi ile birbirleri ile haberleşmesi istenmeyen kullanıcılar gruplara ayrılmış olur. Bu sayede her grup sadece kendi grubundaki yayın etki alanına ulaşabileceği için grup bazlı güvenlik sağlanmış olur. Güvenlik açısından bakılacak olursa, VLAN teknolojisi saldırıların birbirleriyle ilişkili VLAN'lara yayılmasını önlemektedir [11]. Ağda istenmeyen trafik, anahtarların güvenlik özellikleri ve ACL'ler tarafından engellenir. Aynı şekilde tek bir LAN yerine her bir birim için VLAN kullanmak, sorunların etkisini ve LAN'daki tüm son kullanıcılara yönelik saldırıları azaltmak için etkili bir çözümdür.

c) Ölçeklenebilirlik: VLAN'lar yayın bölgelerine göre ayrılmış ağlardır. İhtiyaç duyulan sayıda VLAN anahtarlama cihazlarında oluşturulup, portları istenilen VLAN'ın üyesi yapılabilir. Bunu VLAN kullanmadan yapmaya çalışmanın karşılığı, fiziksel olarak uç noktadan yönlendirici cihaza kadar fiziksel bağlantı yapmaktır.

VLAN oluşturarak sisteme performans ve güvenlik açısından avantajlar sağlansa da, kriterleri oluşturulan VLAN'ların farklı VLAN'larla iletişim kurmasında sıkıntılar yaşanmaktadır [12]. Sıkıntıların giderilmesinde üçüncü katmanda çalışan yönlendiricilere ihtiyaç duyulur. Bu durumda farklı VLAN'lar yönlendirici üzerinden haberleşebilir duruma gelir. Ancak farklı birimler arasındaki tüm iletişim, yönlendirici üzerinden geçmek zorunda olduğundan yönlendiricinin yükü artar. Bununla birlikte yönlendiriciye eklenecek ACL'ler ile iletişimin kontrol altına alınması sağlanır [13], [14].

1.3. VLAN TÜRLERİ

Sanal ağlar oluşturabilmek için çeşitli yöntemler mevcuttur. Bazı anahtarlar temel birtakım yeteneklere sahipken, diğerleri çok daha güçlü özellikler içerdiği için üreticiler kendi anahtar mimarilerine uygun metotlar geliştirmişlerdir. Bu yöntemler aşağıdaki maddelerde verilmiştir [12]:

a) Port tabanlı sanal ağlar: Sanal ağ oluşturmanın en basit yolu olup anahtar portlarının gruplandırılmasıyla oluşturulur. Gruplama işlemi bir anahtar üzerinde olabileceği gibi, birden çok anahtar üzerindeki portlardan da oluşabilir. Port tabanlı sanal ağ tanımları yapıldığında, bir port birden çok sanal ağa üye olamaz. Ayrıca cihazlar yer değiştirdiğinde, yer değiştiren kullanıcı için yeniden yapılandırma işlemi gerekir.

b) Ortam Erişim Yönetimi (MAC- Media Access Control) tabanlı sanal ağlar: MAC kaynak adreslerine göre cihazları sanal ağlara atamak mümkündür. Bu durumda her sanal ağ, bir MAC adres listesidir. MAC tabanlı sanal ağlarda cihaz, bina veya kampüs içinde yer değiştirse bile aynı sanal ağda çalışmaya devam eder.

c) Protokol tabanlı sanal ağlar: Az kullanılan protokol türlerini toparlamak için kullanılan bir yöntemdir. Ancak yaygın olarak kullanılan protokoller için yayın (broadcast) desteği yetersizdir.

d) Kural tabanlı sanal ağlar: En esnek sanal ağ yöntemidir. Kullanıcılar, ağ yöneticisi tarafından belirlenen kurallara göre tanımlanan sanal ağlara bir kez atandıktan sonra, fiziksel yerlerinden bağımsız olarak çalışmalarını sürdürebilmektedir.

1.4. STATİK VE DİNAMİK VLAN

VLAN'lar ağ yöneticisinin ön bilgileri doğrultusunda anahtarlar üzerinde yönetim komutları kullanılarak veya düğümün durumuna göre kendiliğinden olmak üzere sırasıyla statik veya dinamik VLAN olarak iki türde kullanılabilir. Oluşturulan bir VLAN'ın statik ya da dinamik olarak anahtar portlarına atanması gerekir. Bir statik VLAN oluşturulurken ağ yöneticisi anahtarın belirli portlarını VLAN'a dahil eder ve portlar ağ yöneticisi tarafından değiştirilene kadar bu VLAN'ın üyesi olarak kalır. Dinamik VLAN oluşturmada ise, ağ yöneticisi sistemin kurulumu aşamasında ağda bulunan tüm cihazların MAC adreslerini bir yazılım aracılığıyla veritabanına alıp ağdaki adreslerin

VLAN'lara üyeliğini gerçekleştirir. Bu yöntemde MAC adresleri kullanılarak hangi cihazın hangi VLAN'a ait olacağı belirlenir [15]. Dinamik VLAN sisteminde merkezi bir yazılım ve ağa bağlanacak düğümlerin MAC adreslerinin bilinmesi zorunludur.

Dinamik VLAN teknolojisi sayesinde ağ üzerinde bulunan bir son kullanıcının yeri değiştiğinde, yeni gittiği yerdeki anahtar, merkezi MAC veritabanından kullanıcının hangi VLAN'a üye olduğunu bulur ve portu o VLAN'a üye yapar. Böylece fiziksel bir değişiklik yapılmasına gerek kalmadan merkezi yazılımla esnek, alternatif bir çözüm sunulmuş olur. Ayrıca anahtar portlarının ayrı VLAN'lara atanmasıyla her VLAN'a ait porttan yapılan broadcast sadece o VLAN'a ait diğer portlara iletilir. Bu özellik, ağ performansını arttırmanın yanı sıra ağ yönetimi ve güvenliğini de kolaylaştırır. Broadcast trafiği VLAN içerisine hapsolduğundan sistemin görünür bant genişliği artar ve sistemden daha yüksek hızlarda veri akışı sağlanır [16], [17].

1.5. İLGİLİ ÇALIŞMALAR

Dinamik VLAN ile ilgili olarak yapılmış çalışmaların çoğu VLAN'ın yük dengelemesinden çok karmaşıklığı azaltma ve tanımlı düğümlerin aynı sanal ağda bulunmasını esas almıştır.

Koerner ve arkadaşları tarafından yapılan çalışmada mobil kullanıcıların ağın herhangi bir noktasından kendi kaynaklarına erişebilmelerine olanak sağlamak için bir yazılım geliştirilmiştir [18]. Bu yaklaşımda anahtarlama donanımlarının OpenFlow protokolünü desteklemeleri şartıyla cihazların MAC adreslerinin merkezi bir yazılımda toplanarak hangi VLAN'da oldukları tanımlanmakta ve buna göre büyük ölçekli ağlarda düğümler nerede olurlarsa olsunlar kendi yerel kaynaklarının bulunduğu VLAN'a erişimleri sağlanmaktadır.

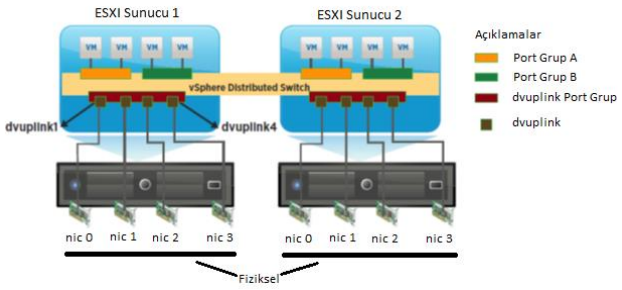
Okayama ve arkadaşlarının yaptığı çalışmada büyük bir yerel alan ağında ortak bir noktadan kendi yerel kaynaklarına erişim sağlamak isteyen kullanıcılar için bir yaklaşım sunulmuştur [19]. Sunulan bu yaklaşımda yerel kaynakları farklı bir VLAN'da olan düğümler ortak bir alanda bağlantı sağladıklarında 3 adet sunucu devreye girerek, kimlik doğrulama yapılmakta şayet doğru ise ortak alanın bağlı olduğu anahtar üzerinde geçici oluşturulmuş VLAN kimlik numarası erişmek istedikleri VLAN kimlik numarası ile değiştirilmektedir. Bu işleri yapan VLAN yöneticisi, VLAN kimlik numarası dönüştürücü ve kimlik doğrulayıcı olmak üzere 3 adet sunucu sistemde görev yaparak

ağda bulunan tüm anahtarlama cihazlarında geçici VLAN kimlik numarası tanımlanmaktadır.

MAC temelli ve yazılım tabanlı kimlik doğrulama kullanılarak yapılan bir diğer çalışmada kullanıcıların, MAC adresleri ağdaki bir yazılımda toplanmış ve ağa erişmek istedikleri nokta neresi olursa olsun Remote Authentication Dial-in User Service (RADIUS) sunucu ile kimlik doğrulaması yapılarak bulunması gerektiği VLAN konfigürasyonu gönderilmesinin doğurduğu sonuçlar analiz edilmiştir [15].

Ning Jiang ve arkadaşlarının çalışmasında ise [20] Cisco'nun kendine özgü MAC bazlı dinamik VLAN yazılımı olan VLAN Management Policy Server (VMPS) ve ağdaki Internet Protocol (IP) telefonlar ile düğümlerin aynı portta kullanılmasını sağlayan ses VLAN'ı uygulaması ele alınmıştır. Cisco'ya özgü VMPS yazılımı, bir ağ yöneticisi tarafından yazılımın veri tabanında bilgisayarların MAC adresleri bulunulması istenen VLAN ile eşleştirilir. Bu sayede ağın neresinden bağlanılırsa bağlanılsın aynı VLAN'da olunmasını sağlayan dinamik VLAN yapısı oluşmaktadır. Bu çalışmada ele alınan ses VLAN'ı ise yine Cisco'ya özgü "Cisco Call Center" santrali ile aralarında olan ve servis kalitesi yüksek sadece ses verisi taşınan bir VLAN'dır.

Vmware sanallaştırma yazılımının kullandığı sanal dağıtık anahtar (VDS-vSphere distributed switch), sanallaştırma ortamlarında yazılım tabanlı ağ (SDN -Software Defined Network-) ve sanal olarak dinamik VLAN kullanarak yük dengelemesi yapmaktadır [21]. Bu teknoloji sayesinde sanal ortamdaki sunucular çoğaltılabilmekte, sunucular arası yük dengelemesi ve uygulama yönlendirmeleri sağlanabilmektedir. Şekil 1.1'de dağıtık anahtar yapısı gösterilmektedir.



Şekil 1.1. Vmware dağıtık anahtar yapısı görünümü [21].

Literatürde yer alan dinamik VLAN uygulamalarının çoğunun amacı kullanıcıların ortama eriştiklerinde kendileri için ayrılmış olan VLAN'a, bağlantı portlarının otomatik olarak üye yapılarak erişmelerini sağlamaktır. Ses VLAN'larına otomatik üye

yapılmalarının sebebi ise ses verilerinin sadece IP telefonların bağlı bulundukları portlara iletilmelerini Cisco'ya özgü geliştirilmiş bir yazılımla sağlamaktır.

Yu-Wei ve arkadaşlarının sistematik VLAN ve erişim kontrol dizayn çalışmasında, ağdaki düğümlerin broadcast trafikleri ve güvenlik seviyelerine göre ağa erişimleri göze alınarak kurumsal bir ağın topolojisini oluşturmaya yönelik bir yaklaşım sunulmuştur. Bu çalışmada dinamik bir yapı olmadığı gibi SNMP protokolü kullanılarak yapılan gerçek zamanlı veri toplama ve ağ cihazlarına konfigürasyon gönderme gibi bir durum söz konusu değildir. Ancak ağ yöneticisine yardımcı olmak amaçlı geliştirilen bu çalışmada, ağı en ideal şekilde broadcast domainlerine ayırmayı ve güvenlik zafiyetlerini geçmeyi hedeflemişlerdir [4].

Abdul Hameed ve arkadaşının yaptığı ağ için en verimli VLAN topolojisinin bulunması üzerine yapılan çalışmada, ağda önceden hesaplanmış trafikler ve bazı 3. parti yazılımlar yardımıyla dinlenilerek elde edilen canlı trafikler üzerinden Simple Set Based algoritması olarak adlandırdıkları bir algoritma geliştirmişlerdir. Algoritmalarını simülasyonda uygulamışlar ve bunun sonucu olarak ağ yöneticisine düğümlerin VLAN üyelikleri için öneride bulunmayı ve ağı daha efektif kullanmayı hedeflemişlerdir [22].

F. Li ve arkadaşlarının çalışmalarına göre; merkezi ve yarı otomatik bir VLAN yönetimi ile ağ yöneticilerinin belirli kısıtlarına göre (örneğin VLAN sayısı) ağdaki cihazlar üzerinde Spanning Tree Protocol'lüne (STP) ihtiyaç duyulmadan VLAN'lar yardımıyla cihazlar arasındaki iletişim kopmadan ve en etkin şekilde VLAN üyeliklerinin sağlanması hedeflenmiştir. Burada SNMP'nin trap mekanizması kullanılarak cihazların trunk portlarının durumları gözlemlenmiş ve düğümlerin, üretebilecekleri trafik değerlerine göre her bir bağlantı topolojisinin optimum trafik değerine ve kullanıcı grubuna göre VLAN'lara üyeliklerine karar verilmeye çalışılmıştır. Cihazlara Secure Shell (SSH) ile bağlanılarak konfigürasyon yollanmış ancak ağın durumu hakkında bilgi edinme seviyesi sadece cihazların uplink portlarının dinlenmesi ile sınırlı kalmıştır [23].

R. Verma ve arkadaşının çalışmasında VLAN kullanılan ağlarda ACL'ler yardımıyla, giriş ve çıkış trafiğini filtrelemek, VLAN atlatma gibi VLAN Trunking Protocol (VTP) sorunlarını gidermek maksadıyla, uç kullanıcıların bağlandığı ve değiştirilmesi en muhtemel olan anahtarların, izinsiz şekilde ağa bağlanmasına karşı koymak amacıyla iletişim için yönlendirici alt arabirimlerin kullanılması önerilmiştir. Önerilen mimari ve VTP simule edilmiş ve analiz sonuçları incelenmiştir. Bu çalışma için Cisco donanım ve

konfigürasyon uygulama yazılımına dayanmaktadır [24].

Kampüs ağlarında birçok VLAN kullanmak, minimal fiber / kablolar üzerinden birçok mantıksal ağın dağıtımı için popüler hale gelmiştir. Örneğin, kampüs çapında bir Wi-Fi sistemi, erişim ağlarını diğer kampüs ağlarından ayırmak ve misafir / ev kullanıcısı ayırma ve güvenlik filtreleme gibi gelişmiş bir erişim kontrolü gerçekleştirmek için çok sayıda VLAN gerekmektedir. Eduroam, yüzlerce uluslararası araştırma ve eğitim kuruluşundan oluşan federasyon üyelerine Wi-Fi dolaşımını sağlayan bir yetkilendirme ve kimlik doğrulama tabanlı bir federasyon altyapısıdır [25]. Özellikle eduroam gibi bir ağ dolaşım sistemi kullanıldığında erişim kontrol listelerini düzenleme gerekliliği çok yüksektir. IEEE 802.1Q'ya [26] dayanan geleneksel VLAN kullanımının bazı sınırlamaları vardır ve sistem yapılandırma çalışması zahmetlidir. Yamasaki ve arkadaşlarının çalışmasında, problemleri çözmek için OpenFlow'a dayalı esnek bir kampüs VLAN sistemi önerilmektedir. Ek olarak, bir prototip sistem tanıtılmış ve değerlendirme sonuçları verilmiştir. Sonuç olarak, önerilen sistemle esnek ağ yapılandırmaları ve gelişmiş erişim kontrolünü çok basitleştirilmiş bir ağ yönetimi çalışmasıyla gerçekleştirebileceği savunulmaktadır [27].

Nagatomo ve arkadaşlarının çalışmasında artırılmış gerçeklik kullanılarak anahtar üzerindeki VLAN yapılandırmasının görsel olarak sunulması hedeflenmiştir. Bu sayede ağ teknisyenleri ve yöneticilerinin fiziksel olarak cihaza bağlanmalarına gerek kalmadan portların VLAN bilgilerine erişilmesi hedeflenmiştir. Bilgiler SNMP vasıtasıyla merkezi bir sunucuda toplanmıştır [28].

Bu çalışmalar dışında bilgisayar ağlarının çeşitli alt alanları ile ilgili literatürde yapılmış çalışmalar da yer almaktadır. Tekerek ve arkadaşlarının yaptığı çalışmada Hyper-Text Transfer Protocol (HTTP) çalıştıran sunuculara erişimdeki atakların sınıflandırılmasına dair bir çalışma gerçekleştirilmiştir [29]. Irmak ve arkadaşının yaptığı çalışmada ise uzaktan erişim sağlanabilen ve yazılımla kullanılabilen bir laboratuvar modellemesi yapılmıştır [30].

Literatürde çok sayıda SNMP kullanılarak yapılmış olan gerçek ve sanal yerel alan ağ topoloji keşif uygulama ve performans artırma algoritmaları da mevcuttur. Bunlardan biri Li Zichao ve arkadaşlarının sanal yerel alan ağ topoloji keşfi [31] diğeri ise Pandey S. ve arkadaşlarının yaptığı LAN'daki topoloji keşifleridir [32].

İki anahtar arasında veya bir anahtardan ağın başka noktalarına birden fazla fiziksel

bağlantı var ise ve bu bağlantılardan biri veya birden çoğu yedek olarak kullanılmak isteniyorsa, paketlerin döngüye girmemesi için anahtarlar üzerinde STP'nin uygulanması gerekmektedir. Şayet bant genişliği kapasitesini arttırmak için iki anahtar arasında birden fazla fiziksel bağlantı kurulmuş ise bu portlar Link Aggregation Group (LAG) olarak ayarlanmalıdır. Ağda birden fazla VLAN ve iki anahtar arasında da birden fazla fiziksel bağlantı var ise, bu bağlantılardan bazıları bazı VLAN'ları taşımak, bazı portları da diğer VLAN'ları taşımak için kullanılıyorsa, bu tip kullanımlara VLAN Load Balancing denmektedir [33]. Ancak bu tez çalışmasında VLAN yük dengelemesinden kastedilen VLAN'lardaki düğümlerin ürettikleri trafik değerlerine göre yük dengelemesi yapmak olduğu için bu konu ile farklılık arz etmektedir.

Bu çalışmada önerdiğimiz SNMP tabanlı dinamik ağ trafiği dengeleme yönteminde ağda bulunan trafiğin durumuna göre VLAN'larda oluşan yükün dengeli bir şekilde dağılımı için kullanıcıların VLAN'larını gerektiğinde değiştirmek ve buna bağlı olarak trafik yoğunluğu birbirine eşit veya yakın yayın bölgeleri oluşturulması sağlanmaktadır. Bu çalışmada sabit VLAN yapısı oluşturulmuş bir ağda, düğümlerin farklı trafik üretmeleri sonucu, aynı güvenlik politikaları uygulanmış VLAN'ların yük dağılımını, VLAN'lara üye düğümlerin dinamik olarak üyeliklerinin değiştirilmesiyle, VLAN trafiklerinin azaltılarak veya artırılarak dengelenmesi sağlanmıştır. Bu yöntem üreticiden bağımsız olarak endüstri standardı olan SNMP protokolünü destekleyen tüm anahtar cihazlarında uygulanabilmektedir. Bu durum, ağ altyapısındaki anahtarların sadece VLAN ve SNMP destekleyen cihazlar olması şartıyla, yeniden bir yatırım yapmak yerine mevcut anahtarlar kullanılarak ek maliyete yol açmayacaktır. Sadece ağ anahtarlarının merkezi bir noktadan yönetimini sağlayacak olan geliştirdiğimiz yazılıma ihtiyaç duyulacaktır. Önerilen yöntemle ağda dinamik olarak VLAN'lar oluşturulabilmekte, portların VLAN'lara üyelikleri dinamik olarak gerçekleştirilebilmektedir. Yönlendirici cihaz kullanma ihtiyacı bulunmadığından mevcut ağ altyapılarında uygulanması ek maliyet getirmemektedir. Ayrıca bu çalışmayla Yazılım Tabanlı Ağların (SDN) ihtiyaç duyduğu özel donanım ve sistemler kullanılmadan, mevcut cihazlar üzerinde dinamik VLAN ile ilgili işlemlerin önerdiğimiz yöntemle gerçekleştirilmesi konusunda literatüre katkı sağlanması hedeflenmiştir.

Bu çalışmanın ikinci bölümünde SNMP'nin çalışması hakkında bilgi verilmiş ve SNMP'de kullanılan Nesne Tanımlayıcılar (OID-Object Identifier) incelenmiştir.

3. bölümde önerdiğimiz VLAN modellemesi ve önerilen yöntemin algoritması üzerinde durulmuş, 4. bölümde ise önerilen yöntemin performans değerlendirmesi yapılmıştır.

2. BASİT AĞ YÖNETİM PROTOKOLÜ

TCP/IP protokol ailesinin bir parçası olan SNMP; ağ yöneticilerinin ağ performansını arttırması, ağ problemlerini bulup çözmesi ve ağlardaki genişleme için planlama yapabilmesine olanak sağlayan bir protokoldür. SNMP sayesinde ağdaki cihazlar izlenebilir, yönetilebilir ve yapılandırmaları değiştirilebilir.

SNMP, basit tasarımından dolayı ağlara kolayca entegre edilebilme, geniş bir kullanım alanına sahip olma ve dağıtık ve merkezi yönetimi destekleme avantajlarına sahiptir [34]. SNMP'nin ağ yönetiminde sağladığı avantajlar ve dezavantajlar Çizelge 2.1'de verilmiştir [35].

Çizelge 2.1. SNMP avantaj ve dezavantajları [35].

	Avantajlar	**Dezavantajlar**
1.	Basit dizaynı kolay entegrasyon sağlıyor.	Düşük güvenlik (son sürüm hariç)
2.	Kullanım alanı çok geniş	User Datagram Protocol (UDP) kullandığından güvenilirlik düşük.
3.	Güncelleme işlemi kolay	Çok fazla ağ trafiği yaratır.
4.	Artan gereksinimlere kolay adaptasyon	
5.	Bir standart olması	
6.	Genişletilebilir ve taşınabilir olması	
7.	Dağıtık ve merkezi yönetimi desteklemesi	

SNMP OSI modelinde Çizelge 2.2'de gösterildiği gibi uygulama, sunum ve oturum katmanlarında çalışmaktadır [35].

Çizelge 2.2. SNMP OSI ve TCP/IP.

OSI	TCP/IP	SNMP
Uygulama Katmanı	Uygulama Katmanı	✓
Sunum Katmanı		✓
Oturum Katmanı		✓
Taşıma Katmanı	Taşıma Katmanı	x
Ağ Katmanı	Ağ Katmanı	x
Veri Bağı Katmanı	Veri Bağı Katmanı	x
Fiziksel Katman		x

2.1. SNMP'NİN GELİŞİMİ

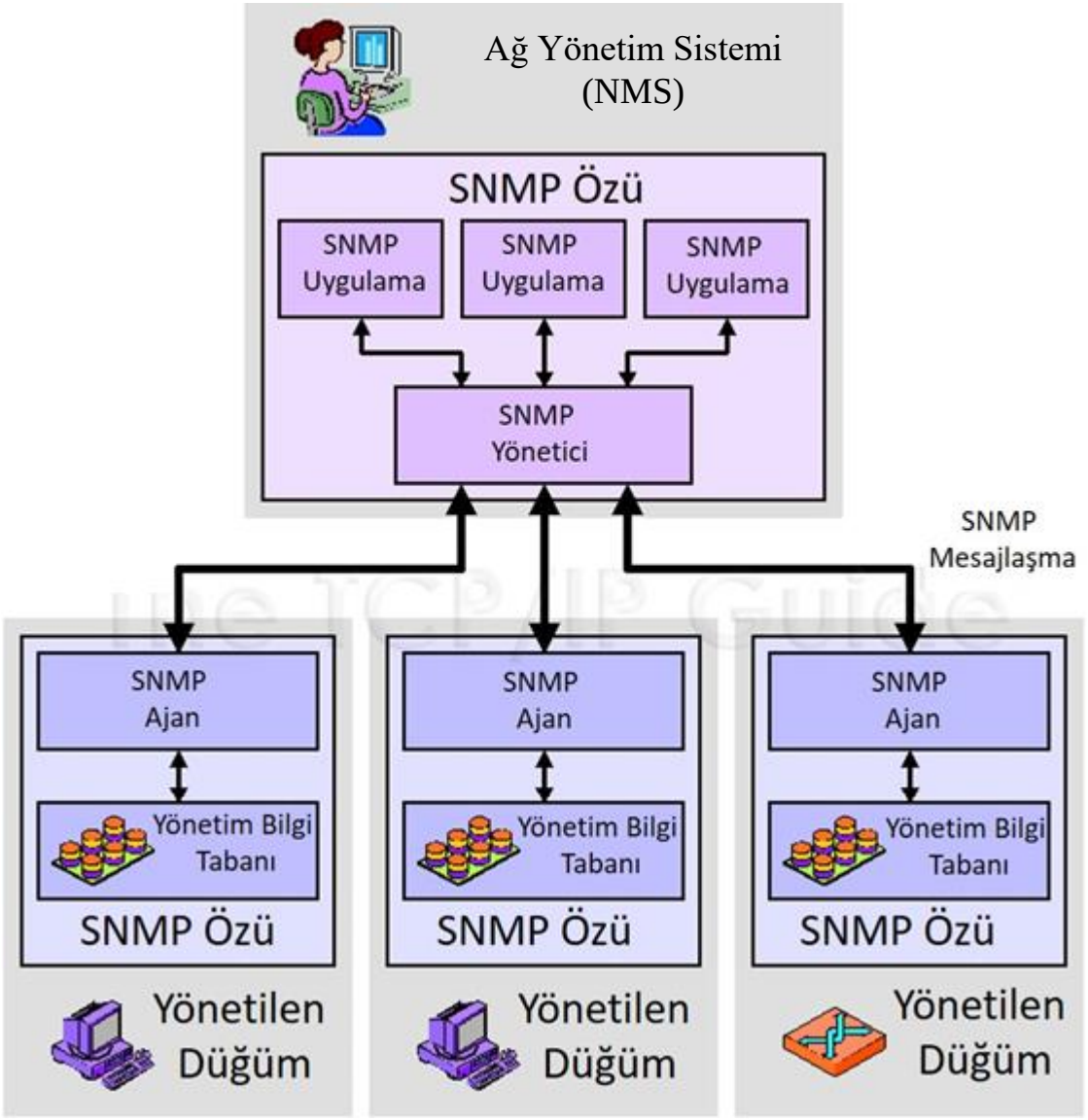
1988 de tasarlandığı haldeki SNMP protokolüne SNMP versiyon 1 (SNMPv1) adı verilmiştir. SNMPv1 beş temel mesaj tipine sahiptir ve mesajların maksimum boyutları kısıtlıdır. Bu eksiklikleri gidermek için 1993 SNMP versiyon 2 ve 1998 yılında SNMP versiyon 3 çıkartılmıştır. İkinci versiyonda cihazlardan veri toplamak için çeşitli yetkilendirme mekanizmaları eklenmiş, versiyon 3 ile birlikte yetkisiz kişilerin ağ cihazlarından bilgi toplamalarını önlemek amacıyla sertifika bazlı kimlik tanımlama yöntemine geçiş yapılmıştır [36]. SNMP versiyonlarının özellikleri ve karşılaştırılması Çizelge 2.3'te [35] verilmiştir. SNMP protokolünün ağ cihazlarını tanımayı kolaylaştırması ve ağ cihazlarını uzaktan kolayca ayarlamayı sağlaması, yaygınlığını artıran ve yaygınlaşmasını sağlayan en önemli etmen olarak söylenebilir [37]. Bu tez çalışmasında güvenlik ve şifreleme açısından daha gelişmiş olduğu için SNMP V3 kullanılmıştır.

Çizelge 2.3. SNMP versiyonları ve karşılaştırması [35].

	SNMPv1	**SNMPv2**	**SNMPv3**
Kullanılan diller	SMIv1	SMIv2	SMIv2
Protokol işlemleri	Get, GetNext, Set	Get, GetNext, GetBulk, Set	Get, GetNext, GetBulk, Set
Özellikler	İlk Standart	SNMPv2-trap,genişletilmiş SMI, yöneticiler arasında iletişim.	SNMPv2-trap, güçlü güvenlik desteği
Standart	1991	1999	1999'dan Sonra
RFC No	1155,1212,1213,1215	1901-1908,2578-2580	2570-2576

2.2. SNMP'NİN MİMARİ YAPISI

SNMP, ajan uygulama, yönetici uygulama ve ağ yönetim sistemi (Network Management System-NMS) bileşenlerinden oluşur [38]. Şekil 2.1'de gösterildiği gibi hiyerarşinin en tepesinde ağ yönetim sistemi bulunmaktadır ve bu sistem ağdaki cihazlardan gelen bilgileri yorumlayan yazılımdır. Orta seviyede ise ağı dinleyen ve ağa yönetim bilgilerini gönderen yönetici uygulama bulunmaktadır. En alt seviyede ise ağdaki uç cihazlardan gelen sinyalleri yönetici uygulamaya gönderen ajan uygulama bulunmaktadır.



Şekil 2.1. SNMP mimarisi [39].

2.2.1. Ajan Uygulama

Ajan uygulama, SNMP hizmetini ağ cihazı üzerinde çalıştırıp gerekli bilgileri kayıtlı tutarak yönetici birime aktarma veya yönetici birimden gelen değişiklik isteklerini cihaza uygulama görevlerini yerine getirir. Ağdaki uç cihazlarda bu özelliğin bulunması ve aktif hale getirilerek, hangi yönetici uygulamaya (IP adresi) veri göndereceği ve hangi SNMP versiyonunu kullanacağı bilgisinin girilmesi gerekmektedir. Bu bilgiler arasında kimlik doğrulama bilgilerinin de bulunması zorunludur.

2.2.2. Yönetici Uygulama

Yönetici uygulama, ajan uygulamadan ihtiyaç duyulan bilgileri alıp kullanıcıya görüntüleme ve kullanıcının değiştirmek istediği değerleri ağ cihazına gönderme görevlerini yerine getiren yazılımdır. Ajan uygulama çalışan uç cihazdan ihtiyaç duyulan bilgileri ve aynı şekilde değiştirilmek istene değerleri uç cihaz ile aralarında oturumlar açarak gönderir ve alır [40], [41]. Ajan uygulamada olduğu gibi Yönetici uygulamanın da ağ yönetim sisteminde ağı dinleyecek şekilde ayarlanarak hangi SNMP versiyonu kullanacağı ve kimlik doğrulama bilgilerinin girilmesi gerekmektedir.

2.2.3. Ağ Yönetim Sistemi

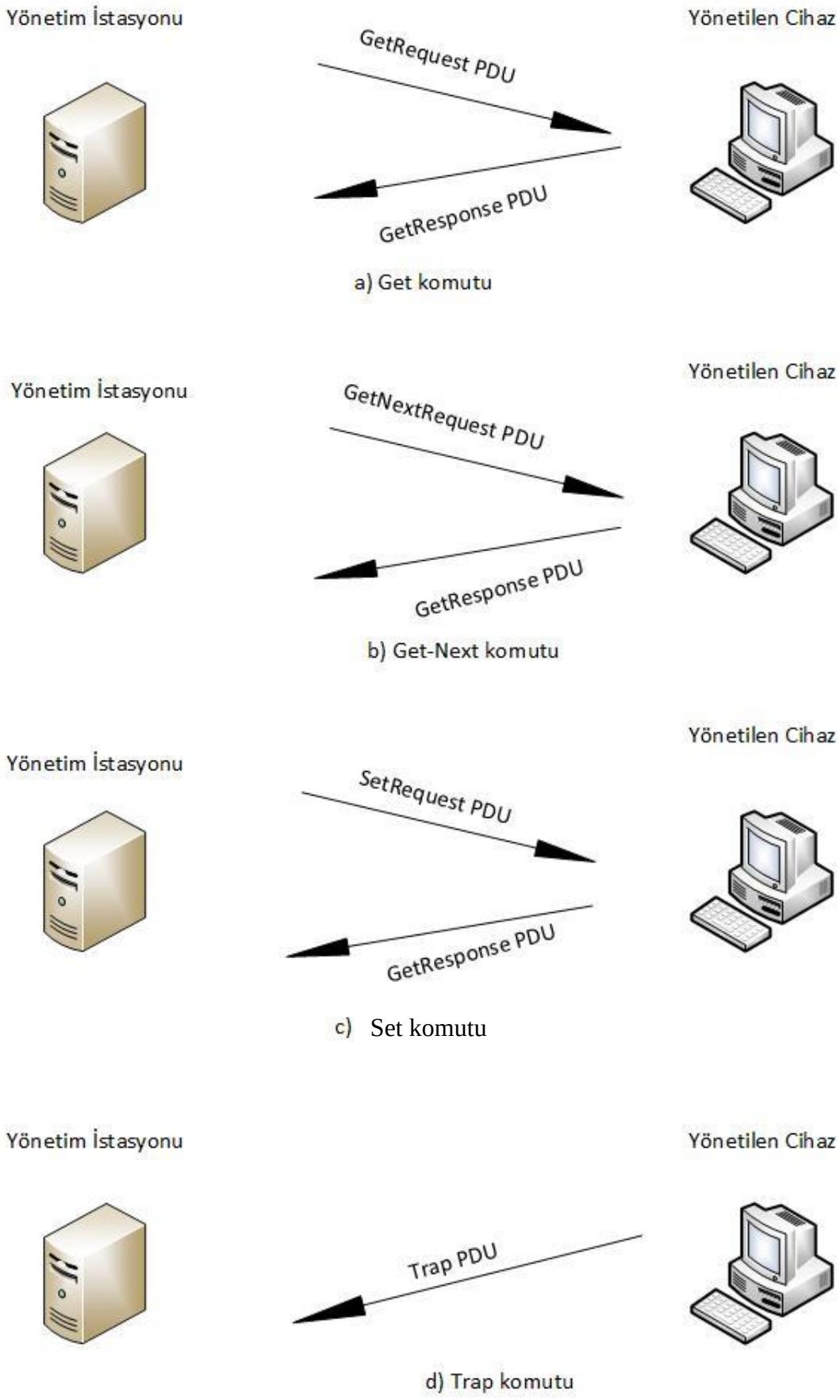
Ağ Yönetim Sistemi (NMS) Şekil 2.1'de gösterildiği gibi, yönetici birimde çalışan ve bir ağa bağlı tüm cihazların izlenmesini ve yönetimini sağlayan uygulamadır. Bu uygulama ağdaki uç cihazlardaki bilgileri analiz etmede ve gerekliyse bu cihazlarda konfigürasyon değişikliği yapma gibi görevleri üstlenmektedir.

2.3. SNMP İLETİŞİMİ

SNMP uç cihaz ile ilgili belirli bilgileri, bağlı bulunduğu anahtar üzerinden yönetim sistemine, belirli standartlar ve belirli kurallar çerçevesinde iletilmesini sağlar. Bu kurallar, sıralamalar ve standartlar aşağıda detaylı olarak verilmiştir.

2.3.1. SNMP Paket Sırası

Ağda üzerinde ajan uygulaması çalışan uç cihazlar ve yönetici uygulaması çalışan yönetim sistemi arasında SNMP paketleri Şekil 2.2'de gösterildiği sıra ile gönderilip alınmaktadır [41].



Şekil 2.2. SNMP paket sırası [41].

Öncelikle yönetilmek istenen cihaza get komutu ve parametreleri ile sorgu gönderilir. Daha sonra üzerinde ajan uygulama çalışan cihaz buna cevap döner. GetNextRequest ile sıradaki bilgi sorularak uç cihazdan sıradaki bilginin dönmesi sağlanır, sıradaki bilgiden kasıt ileriki bölümlerde anlatılacak olan MIB ağacında bir sonraki değer demektir. Set işlemi ise üzerinde değişiklik yapılmak istenilen cihaza değişiklik için parametre ve komut gönderilmesinin sağlar ve buna uç cihazın cevabı olumlu ya da olumsuz olarak geri dönmektedir. Son olarak trap mekanizması ise şu şekilde işlemektedir:

Uç cihaz üzerinde ayarlanmış olan yönetici adresine kendinde olan değişiklikleri komut ve parametre vasıtası ile göndermektedir. Örneğin "fiziksel bir porta bir cihaz bağlandı" ya da "port bağlantısı kesildi" vb.

2.3.2. SNMP Paket Yapısı

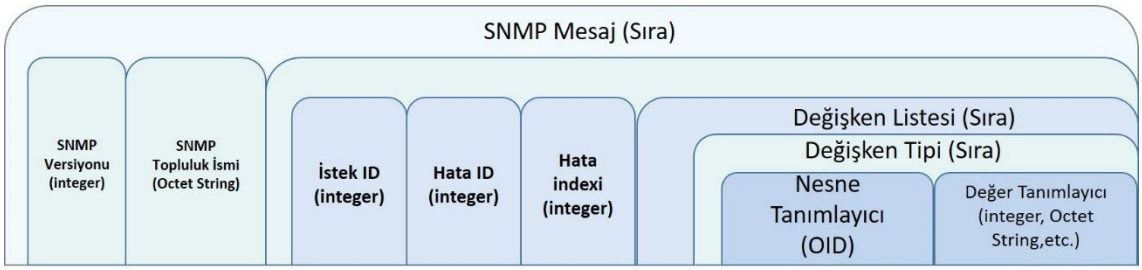
SNMP bileşenlerinin iletişimi için UDP protokolü kullanılır. UDP'nin karakteristiklerinden dolayı, iletişim verilerinin başlık yükü düşük olup, sıralama, akış kontrolü ve oturum kurma işlemleri gerçekleştirilmez. Bu sayede çok hızlı iletişim gerçekleşir. SNMP'nin üçüncü sürümü ile birlikte şifreli veri iletişimi ve kimlik doğrulama özellikleri sayesinde güvenlik ön plana çıkarılmış ve önceki sürümlerde olan dezavantajlar ortadan kaldırılmıştır [42].

SNMP paketi SNMP mesajı ve Protokol Veri Ünitesi (PDU- Protocol Data Unit) olmak üzere Şekil 2.3'te gösterildiği gibi iki yapıdan oluşur [43].

Mesaj Başlığı	PDU

Şekil 2.3. SNMP paket yapısı [43].

SNMP paketi içindeki alanlar sırasıyla Şekil 2.4'te detaylı bir şekilde verilmiştir [44].



Şekil 2.4. SNMP paket içeriği [44].

SNMP versiyon numarası iletişimin hangi SNMP versiyonu ile yapılacağını, SNMP

topluluk ismi ise bir kimlik doğrulama mekanizması gibi çalışmaktadır [35]. Aşağıda verilen Çizelge 2.4'te paket içeriği boyutları ile beraber detaylı bir şekilde açıklanmıştır [45].

Çizelge 2.4. SNMP paketi boyut ve içeriği [45].

Alan Adı	**Açıklama**	**Boyut**
SNMP Mesajı	SNMP sürümünü, topluluk ismini ve SNMP PDU'sunu belirten SNMP mesaj sırasını belirtir.	2 byte
SNMP Sürümü	Hangi sürümün kullanıldığını belirtir.	3 byte
SNMP Topluluk ismi	SNMP cihazlarına güvenlik ekleyebilmek ve onlara kolay erişebilmek için tanımlanan octet string'dir.	8 byte
SNMP PDU	SNMP mesajının ana bölümünü oluşturur. Farklı protokol veri birimlerini (PDU) tanımlar. Aşağıda SNMP V3 PDU'su ayrıca açıklanacaktır	2 byte
İstek ID	Belirli SNMP isteklerini tanımlar. Bu index, SNMP yöneticisine uygun isteğe dönen cevabı eşleştirme izni verir, SNMP ajan yazılımdan dönen cevabın yansıması gibidir.	3 byte
Hata Durumu	SNMP yöneticisinden gönderilen isteğe 0x00 değeri atanır. Sistemde bir hata varsa SNMP ajanı bu alanı değiştirir. 0x00—Hata yok 0x01—Dönen cevap aktarım için büyük. 0x02—İstenen nesne bulunamadı. 0x03—istekteki veri tipi, SNMP ajanındaki veri tipiyle eşleşmiyor. 0x04— SNMP yöneticisi sadece okuma parametresi atadı. 0x05—Genel Hata	3 byte
Hata İndeksi	Hata olursa, hataya neden olan nesne işaretlenir, diğer taraftan hata indeksi 0x00	3 byte

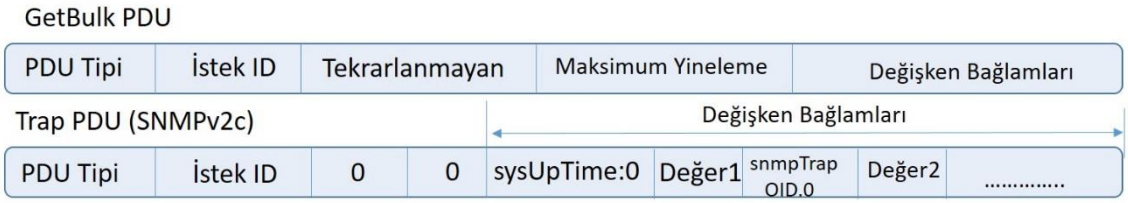
Çizelge 2.4. (devam). SNMP paketi boyut ve içeriği.

Alan Adı	Açıklama	Boyut
Değişken Listesi	Bu alanda SNMP PDU çeşidine göre veya uygulama alanına göre farklı değişkenler alabilir.	2 byte
Değişken Tipi	İki alandan oluşur. OID ve OID'nin değeri	2 byte
Nesne Tanımlayıcı (OID)	SNMP ajanındaki parametreleri ifade eder.	12 byte
Değer	SetRequest PDU – Değer, SNMP ajanındaki belirtilen OID'ye atanır. GetRequestPDU – Değeri boştur, dönen verinin izi gibi davranır. GetResponsePDU – SNMP ajanından belirtilen OID'den dönen değerdir.	2 byte

SNMP Komutlarına göre şekillenen paket yapıları SNMP versiyonlarına göre Şekil 2.5, Şekil 2.6 ve Şekil 2.7'de V1, V2 ve V3 için sırayla verilmiştir.



Şekil 2.5. SNMPv1 PDU çeşitleri [46].



Şekil 2.6. SNMPv2 PDU çeşitleri [47].



Şekil 2.7. SNMPv3 PDU mesaj yapısı [47].

SNMPv3 mesaj içeriğinde PDU SNMPv1 ve SNMPv2'de olduğu gibidir. Ancak Mesaj başlığı güvenlik için farklılaşmış ve ek bilgiler içerecek şekilde Şekil 2.7'de gösterildiği gibi güncellenmiştir.

SNMPv3 mesaj başlığındaki alanlar Çizelge 2.5'te detaylı olarak verilmiştir.

Çizelge 2.5. SNMPv3 mesaj başlık alanları [47].

Alan Adı	**Açıklaması**
Maksimum Boyut	Gönderilen maksimum mesaj boyutu
Bayraklar	0x0 - Doğrulama ve gizlilik yok 0x1 – Doğrulama var, gizlilik yok 0x3 – Doğrulama ve gizlilik var 0x4 – Bir tane PDU raporu gönderir.
Güvenlik Modeli	Güvenlik modelini ifade eder. 0 – Güvenlik modeli yok. 1-SNMPv1 güvenlik modeli 2-SNMPv2c güvenlik modeli 3-SNMPv3 güvenlik modeli
Bağlam Motor ID	Her işlem için özgün bir SNMP girdisi tanımlar.

Çizelge 2.5. (devam). SNMPv3 mesaj başlık alanları.

Alan Adı	**Açıklaması**
Bağlam Adı	İçerik ismi tanımlar. Her isim içeri motor ID ile eşleştirilmelidir. • AuthoritativeEngineID: Kimlik doğrulama ve şifreleme için kullanılan mesaj alışverişinde bulunan yetkili SNMP motorunun snmpEngineID'sini belirtir. Bu alan, bir tuzağı, yanıtı veya raporu ve Get, GetNext, GetBulk veya Set işlemi için hedef kaynağını belirtir. • AuthoritativeEngineBoots: İletinin değişiminde yer alan yetkili SNMP motorundaki snmpEngineBoots değerini belirtir. İlk yapılandırmasından beri bu SNMP motorunun kendisini başlatıp başlatmadığını gösterir. • AuthoritativeEngineTime : İletinin değişiminde yer alan yetkili SNMP motorundaki snmpEngineTime değerini belirtir. Zaman penceresi kontrolü için kullanılır. • UserName : İletisinin değiştirildiği kullanıcıyı (asıl) belirtir. NMS ve Agent üzerinde yapılandırılmış kullanıcı adları aynı olmalıdır. • AuthenticationParameters : Kimlik doğrulama hesaplamasında kullanılan bir anahtar. Kimlik doğrulama yapılmazsa, bu alan boştur.
Güvenlik Parametre	Gizlilik hesaplamasında kullanılan bir parametredir. Örneğin, DES CBC algoritmasında başlatma vektörünü (IV) oluşturmak için kullanılan değer. Herhangi bir gizlilik kabul edilmezse, bu alan boştur.

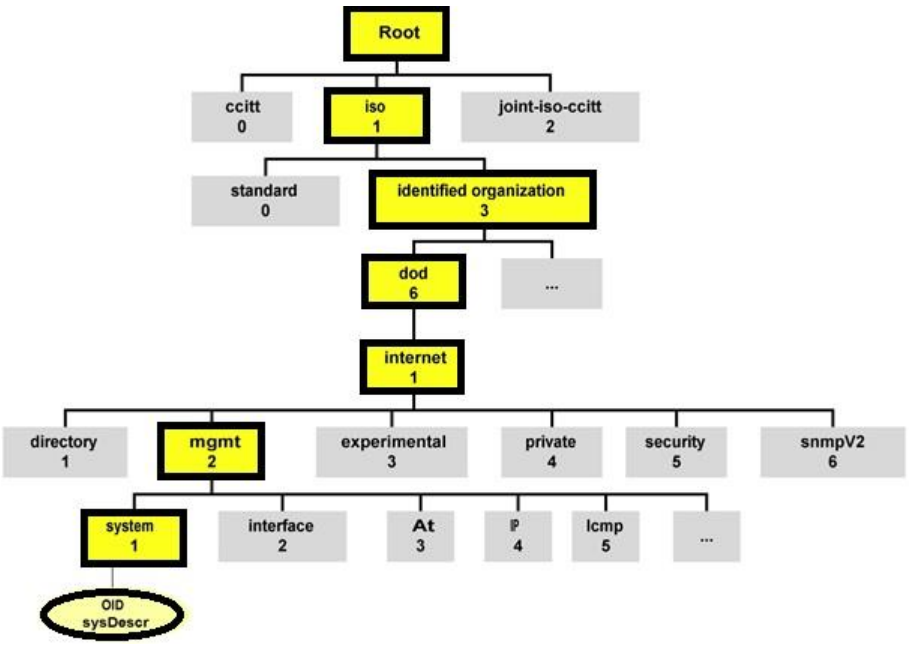
Bu tez çalışmasında güvenlik ve şifreleme özelliklerinde dolayı SNMP V3 tercih edilmiştir.

2.3.3. MIB ve OID Kavramları

SNMP'nin işleyişinde iki kavramı ön plana çıkarmak gerekir. Bunlar Yönetim Bilgi Tabanı (Management Information Base-MIB) [48] ve OID'dir [49]. MIB, her cihazın yerelinde bulunan, cihazdaki ajan uygulama tarafından erişim sağlanan ve cihazla ilgili bilgileri bulunduran bir veri tabanıdır. SNMP'nin çalışma mekanizması istek gönderme ve isteğe cevap alma şeklindedir. İstekler ve cevapları UDP ile gönderilip alınır. Yönetim

sunucusu istekleri herhangi bir portundan ajanın 161. portuna gönderir. İletişimi ajanın başlatması durumunda bildirimler yönetim sunucusunun 162. portuna gönderilir [49]. SNMP sayesinde bir cihazdan bilgi alınabileceği gibi, cihazdaki bilgi değiştirilebilir ve cihazda yeni bir yapılandırma uygulanabilir. Örneğin cihaz yeniden başlatılabilir, cihaza bir yapılandırma dosyası gönderilebilir ya da cihazdan alınabilir.

MIB kavramı Şekil 2.8'deki gibi bir ağaç yapısına benzetilebilir. Ulaşılmak istenen değeri tutan değişken OID'dir [50]. Bu değişkenler ağacın dallarının en uç noktasında olup bir cihazla ilgili tek bir değeri tutabileceği gibi kendisinden sonra gelen bütün alt dalları ifade etmek için de kullanılabilirler. Kökten ağaç dalına uzanan bu hiyerarşi birbirlerinden nokta ile ayrılmış sayı dizileriyle ifade edilir.



Şekil 2.8. MIB ağaç yapısı OID numaraları [50].

Örneğin 1.3.6.1.2.1 ifadesinde yer alan noktayla ayrılmış değerler soldan sağa doğru sırasıyla; 1 : ISO (International Standart Organization), 3 : Org (organization), 6 : Dod (Department of defense), 1 : Internet, 2 : Mgmt (Network management entries), 1: System. Değişkenin başındaki ilk dört değer olan 1.3.6.1 standarttır. Bu noktadan sonra ulaşılmak istenen bilgiye göre alt dallara ilerlenir. Örneğin 1.3.6.1.2.1.1 dalı (sysDescr) sistemle ilgili sistem adı, sistem tanımı, sistemin ayakta olduğu süre gibi değerleri tutar. Bunun alt dalı olan 1.3.6.1.2.1.1 değişkeni bunlardan biridir.

2.4. SNMP VE C#

Algoritmanın test ortamını hazırlamak için Microsoft firmasının Visual Studio 2017 ürününün C# yazılım dili tabanlı ve veri tabanı olarak yine aynı firmanın MS-SQL 2014 programını kullanan bir yazılım geliştirilmiştir.

C# kodlaması esnasında yazılımın SNMP ile mevcut ağın dinlemesi ve aynı zamanda algoritma gereği gerekli değişiklik parametrelerinin anahtarlara yollanabilmesi için C# kütüphanelerinden Çizelge 2.6'de verilen C#'ın kendi bünyesinde ve dış kaynak kodlu SnmpSharpNet [51] isimli hazır kütüphaneler kullanılmıştır.

Çizelge 2.6. SNMP için kullanılan hazır kütüphaneler

SNMP ve MultiThreading Kütüphaneleri	
C# Hazır Kütüphaneleri	System.Net, System.Threading, System.Net.Sockets.
Dış Kaynak Kodlu Hazır Kütüphane	SnmpSharpNet.

Burada dikkat edilmesi gereken hususlardan birisi yazılım ağdaki anahtarlara konfigürasyon gönderirken aynı zamanda SNMP'nin trap mekanizması ile anahtarlardan gelen bilgileri yorumlayıp gerekli işlemleri yapabilmesidir. Bu ise multithreading denilen tek bir program için eş zamanlı ilerleyen prosedürler veya yordamlar ile gerçekleştirilebilir. Yazılımda ağı sürekli dinleyen ve bir trap bilgisi geldiğinde yorumlayan bir fonksiyon bulunmaktadır. Süresi ayarlanabilen ve belirli aralıklarla çalışan, VLAN üyeliklerine karar veren algoritma ayrı bir fonksiyon, yeni bir VLAN oluşturulması için gerekli karar veren algoritma ayrı bir fonksiyon olarak yazılmıştır.

2.5. ANAHTARLARDA SNMP KONFİGÜRASYONU

Yazılımın anahtarlarla iletişimi esnasında şifreli haberleşme ve kimlik doğrulama mekanizmaları kullanıldığı için SNMPv3 ayarlamalarının ve IP yapılandırmalarının anahtarlarda yapılması gerekmektedir. Yöneticinin belirlediği kullanıcı adı ve şifresi düğüm bağlanılacak seviyede her anahtara girilmesi gerekmektedir. Buradaki kısıt ise yazılımın bu algoritmayı gerçekleştirebilmesi için SNMP komutlarının tüm üreticilerde aynı olmasına karşılık, anahtarlarda SNMP konfigürasyonunun mutlaka bir ağ yöneticisi

tarafından yapılandırılması gerekmektedir. Anahtarlarda yapılması gereken konfigürasyon ayarları ise şunlardır;

a. Anahtara IP adresi atama.
b. Anahtarda SNMPv3 versiyonu ayarlanması.
c. Anahtarda SNMP kimlik doğrulama için kullanıcı adı şifre girilmesi.
d. Anahtarda SNMP yönetici IP adresi atanması.
e. Anahtarda, kullanılacak olan bütün VLAN'ların tanımlanması.
f. Anahtarda bütün portların varsayılan VLAN'a üye yapılması.
g. Anahtarlarda, uplink portlarının VLAN'ları etiketli olarak taşıyabilecek şekilde ayarlanması.

3. SNMP İLE DİNAMİK VLAN MODELLEMESİ

Bu bölümde çalışmada kullanılan yöntemin matematiksel ifadeleri algoritmaları akış diyagramları detaylı bir şekilde verilmiştir.

Bu çalışmada VLAN'lar ile yayın bölgelerine ayrılmış yerel alan ağlarında, düğüm sayısına bakmaksızın her bir VLAN'daki toplam trafiğin birbirine eşit veya yakın yapılması amaçlanmaktadır. LAN'da eşdeğer güvenlik seviyesine sahip VLAN'ların üye düğümlerin ürettikleri trafiklere göre dinamik olarak üyeliklerinin değiştirilmesi ile, VLAN'ların yayın trafiği dengelenmeye, buna bağlı olarak da VLAN'lardaki üye düğümlerin ağa erişimlerindeki gecikmelerin azaltılması hedeflenmiştir.

3.1. MATEMATİKSEL MODELİ VE EŞİTLİKLERİ

Teorik olarak bir ağa ait gecikme süresi ile throughput değerlerinin birbirinden bağımsız olması gerekmektedir. Ancak pratikte bu iki terim arasında bir ilişki vardır. Paket kuyruğu hâlihazırda dolu olan bir yönlendiriciye yeni bir paket geldiğinde, kuyruğun en arka sırasına koyulacak ve önündeki paketlerin iletimi tamamlanıncaya kadar kuyrukta bekletilmesi gerekecektir. Dolayısıyla trafik yoğunluğu olması durumunda paketlerin yola giriş süresi daha uzun olacaktır. Bu bağlamda gecikme süresi oranı Denklem (3.1)'de verilen formülle hesaplanmaktadır;

$$D = \frac{D_0}{(1 - U)} \tag{3.1}$$

Denklem (3.1)'de verilen formülde D efektif gecikme süresi, D_0 ağın kullanılmadığı andaki gecikme süresi ve U ise ölçüm yapıldığı andaki aktif kullanım oranını gösteren 0 ile 1 arasında değişen bir değerdir.

Ağ boş iken U değeri 0 olacak ve efektif gecikme süresi D_0 değerine eşit olacaktır. Ağ aktif kullanım oranı yarı kapasitede olacak şekilde arttırıldığında ise efektif gecikme süresi iki katına çıkacaktır. Trafik ağ kapasitesine yaklaştığında ise (yani U değeri 1 olduğunda) gecikme süresi sonsuza ıraksayacaktır. Bu nedenle ağ yöneticileri ağ aktif kullanım oranını sürekli düşük tutabilmek isterler ve bu amaçla ağ trafiğini devamlı

olarak kontrol ederler. Ağın aktif kullanım oranı üst ya da ortalama sınırı aştığında ağ yöneticileri ağı sanal ağlara bölmek suretiyle bu oranı düşürmeye çalışmaktadırlar [52].

Bu çalışmada önerdiğimiz yöntemde ağ aktif kullanım oranını dolayısıyla gecikme süresini düşük tutmak amacıyla SNMP'den yararlanılmıştır. VLAN trafiğinin seviyesi ile ilgili olarak tanımlanabilir veya öndeğerli bir eşik değeri kullanılmıştır. Şayet VLAN trafikleri bu eşik değerini aşarsa sistem öntanımlı olarak hâlihazırda tanımlanmış olan VLAN'ları kullanmaya başlar ve düğümler için bu VLAN'lar aktifleştirilir. Örneğin mevcut kullanılan VLAN'ların toplam trafiği eşik değerini aşarsa kullanıma açık olmayan fakat IP adres havuzu ve omurga anahtar üzerinde gerekli yönlendirmeleri yapılmış olan VLAN kullanıma alınır. Düğümler bu yeni VLAN'a üye olabilirler.

Geliştirilen algoritmada i adet VLAN'a ait bilgileri tutmak için ix3 boyutlu ve Denklem (3.2)'de verilen VLAN adlı matris oluşturulmuştur.

$$VLAN = \begin{bmatrix} id_1 & tt_1 & gd_1 \\ id_2 & tt_2 & gd_2 \\ \text{M} & \text{M} & \text{M} \\ \text{M} & \text{M} & \text{M} \\ id_i & tt_i & gd_i \end{bmatrix} \tag{3.2}$$

Denklem (3.2)'deki id_i, VLAN tanımlayıcı numarasını, tt_i, i. VLAN'ın toplam trafiğini ve gd_i, VLAN'ın güvenlik düzeyini belirtmektedir.

VLAN'lara üye olacak j adet düğüme ait bilgileri tutmak için Denklem (3.3)'te verilen jx6 boyutunda D adlı matris oluşturulmuştur.

$$D = \begin{bmatrix} mac_1 & sip_1 & sp_1 & v_1 & tr_1 & gd_1 \\ mac_2 & sip_2 & sp_2 & v_2 & tr_2 & gd_2 \\ \text{M} & \text{M} & \text{M} & \text{M} & \text{M} & \text{M} \\ \text{M} & \text{M} & \text{M} & \text{M} & \text{M} & \text{M} \\ macj & sip_j & sp_j & v_j & tr_j & gd_j \end{bmatrix} \tag{3.3}$$

Denklem (3.3)'teki değerler sırasıyla mac_j, j. düğümün mac adresini, sip_j, bulunduğu anahtarın ip adresini, sp_j, anahtardaki port numarasını, v_j, üye olduğu VLAN tanımlayıcı numarasını, tr_j, düğümün ürettiği trafiği, gd_j, üye olduğu VLAN'ın güvenlik düzeyini ifade etmektedir. Burada dikkat edilmesi gereken husus VLAN matrisindeki id_i değişkeni

kullanılan VLAN'ın tanımlayıcı numarası, D matrisindeki v_j değişkeni ise düğümlerin üye oldukları VLAN'ın tanımlayıcı bilgisidir.

Algoritmaya göre en yüksek trafik üreten düğümler sırasıyla VLAN'lara dağıtıldıktan sonra, VLAN sayısından fazla olan düğümler son VLAN'dan başlayarak VLAN'lara eklenir (3 adet VLAN varsa 4. düğüm 3. VLAN'a 5. düğüm 2. VLAN'a üye olacak şekilde). Bir düğümün ürettiği trafik şayet ekleneceği VLAN'dan önceki VLAN trafiğinden küçük veya eşitse o VLAN'a üye olur. Aksi halde bir önceki VLAN'a üye olma aşamasına geçer ve bu kontrol tekrar edilir. k. VLAN'ın toplam trafiği Denklem (3.4)'te verilen ifade ile hesaplanır:

$$\mathrm{tt}_k = \begin{cases} \sum_{k=0}^{i} \mathrm{tr}_n, & \mathrm{V}_n = k \\ 0, & \mathrm{V}_n \neq k \end{cases} \tag{3.4}$$

Denklem (3.4)'te verilen V_n, n. düğümün VLAN üyeliğini ifade etmektedir.

Düğümlerin VLAN üyeliklerinin belirlenmesi için aşağıdaki ifade kullanılmalıdır:

l. düğümün VLAN üyeliği Denklem (3.5)'te verilen ifade ile elde edilir:

$$\mathrm{V}_l = \begin{cases} k, & \mathrm{tt}_k + \mathrm{tr}_l < \mathrm{tt}_{k-1} \\ k-1, & \mathrm{tt}_k + \mathrm{tr}_l \geq \mathrm{tt}_{k-1} \end{cases} \tag{3.5}$$

Denklem (3.5)'te k: VLAN kimlik numarasını, ttk: k. VLAN'ın toplam trafiğini ve trl ise l. düğümün ürettiği trafiği temsil etmektedir. Denklem (3.4) ve Denklem.(3.5)'te verilen ifadeler kullanılarak belirlenen VLAN üyelik işlemlerini kullanan algoritmanın akış diyagramı Şekil 3.2'de, sözde kodu Sekil 3.5'te verilmiştir. İlk VLAN ile karşılaştırma yapılana kadar döngü devam eder. Bu süreçte şart sağlanmazsa düğüm ilk VLAN'a üye yapılır. Böylece her bir VLAN'daki ağ trafiği yükü dengeli olarak dağıtılmış olmaktadır. Ağın yoğun kullanımlarında VLAN sayısını dinamik olarak arttırmak için kullanılan algoritmanın akış diyagramı Şekil 3.1'de sözde kodu Şekil 3.4'te verilmiştir. VLAN sayısının dinamik olarak arttırılması, kendisine üye olan düğümlerin toplam trafikleri algoritmada belirtilen eşik değerinin üzerine çıktığı zaman, önceden ağda tanımlanmış fakat pasif konumdaki VLAN'ı aktifleştirerek VLAN dağıtım algoritmasının tekrar çağrılmasıyla gerçekleştirilir. Bu işlem için gerçek zamanlı bir ağ kurulmuş olup sonuçları Bölüm 4'te yer alan Senaryo 5'te verilmiştir. Ağın aktif kullanımı esnasında

ağa dahil olan bir düğümün yeni bir düğüm olup olmadığı kontrolü ve üyelik bilgisi karar algoritması için akış diyagramı Şekil 3.3'te verilmiş olup bu durumu değerlendiren bir senaryo Bölüm 4- Senaryo 4'te verilmiştir.

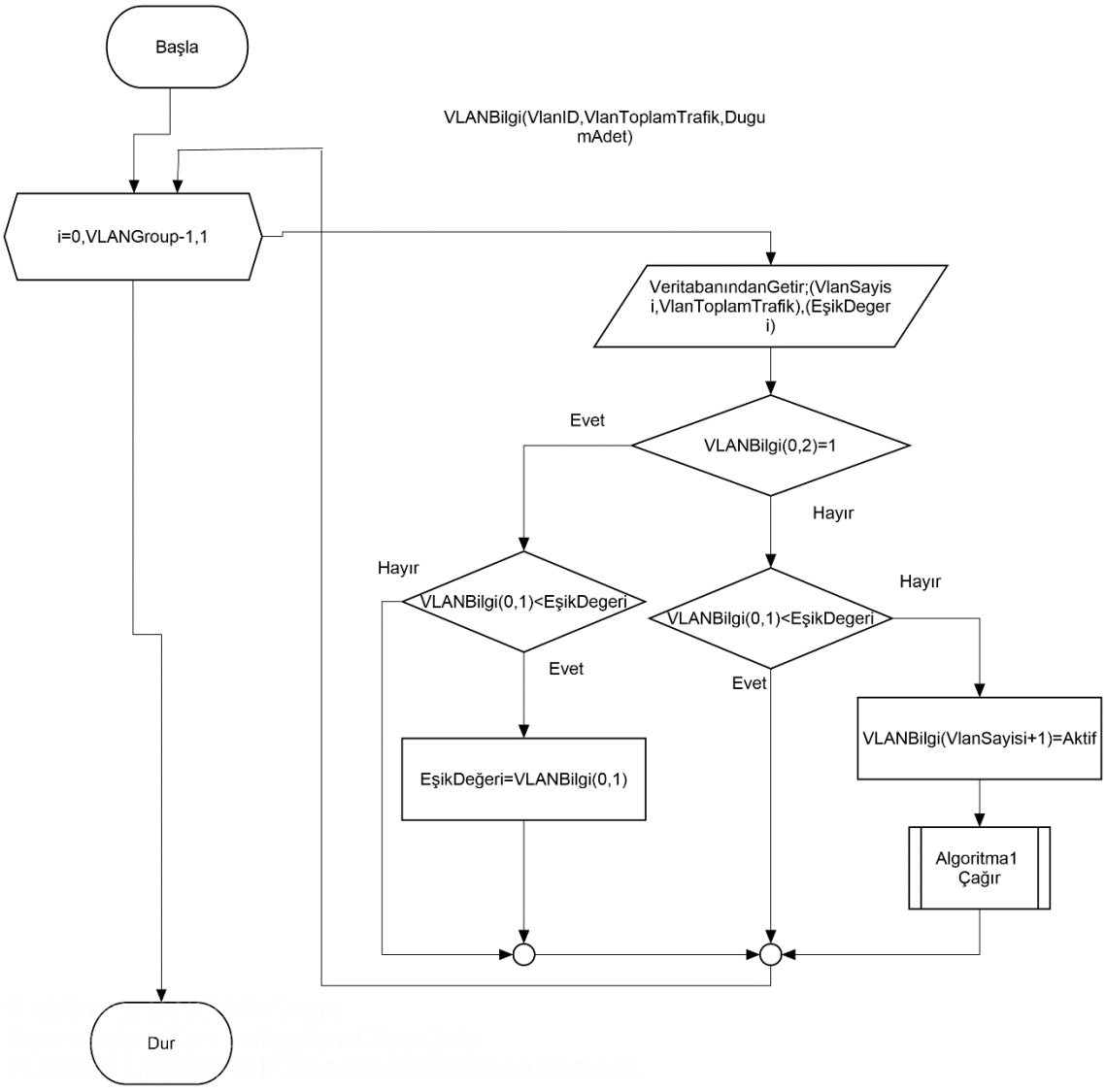
Bu tez çalışmasında geliştirilen algoritma için aşağıda maddeler halinde verilen kabuller olmak zorundadır.

1. Kabul: Güvenlik düzeyi farklı VLAN'lar yazılımda tanımlanmıştır.
    - Gerekçe: Algoritmada kaç adet farklı güvenlik düzeyli VLAN olmasına karar veren bir mekanizma yoktur. Bu ağ yöneticisinin kararı ve yetkisinde olan, yazılımda değiştirilebilen bir parametredir.
2. Kabul: Farklı güvenlik düzeyine sahip VLAN'lara üye düğümlerin MAC adresleri yazılımla veritabanına kaydedilmiştir.
    - Gerekçe: Hangi düğümün hangi güvenlik düzeyinde ağa erişeceği ağ yöneticisinin kontrolünde olmalıdır.
3. Kabul: Eşik değerleri yazılımla veritabanına kaydedilmiştir.
    - Gerekçe: Algoritma ağın hangi trafik yoğunluğunda dinamik olarak yeni bir VLAN ekleyeceğine karar verebilmesi için bu değer baştan girilmeli ya da sonradan değiştirilebilir olmalıdır.
4. Kabul: Algoritmanın çağrılma zaman aralıkları yazılımda tanımlanmıştır.
    - Gerekçe: Dinamik bir yapıya sahip VLAN'ın, sıklıkla kontrol edilip düğümlerin üyeliklerinin değiştirilmesi çok istenen bir durum değildir. Bu işlemin ağ yöneticisinin karar verdiği belirli zaman aralıklarında gerçekleştirilmesi önemlidir. Bu da parametrik bir değerdir.

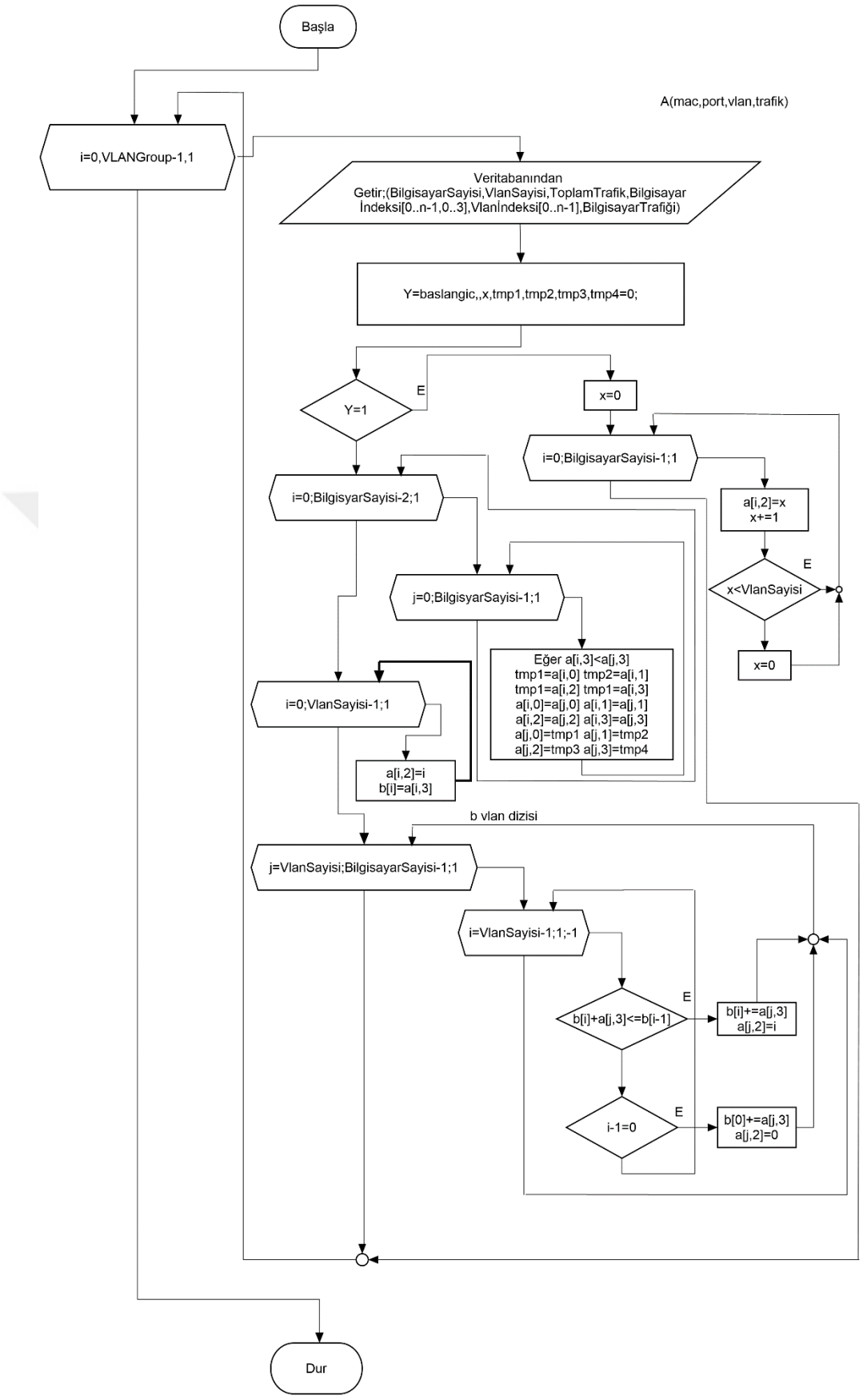
3.2. ALGORİTMA VE AKIŞ DİYAGRAMLARI

Önerdiğimiz yöntem, iki aşamada işlem gerçekleştirilen algoritmalardan oluşmaktadır. Birinci aşamada ağ için gerekli olan VLAN ekleme işlemini yapan ve Şekil 3.1'de akış diyagramı, Şekil 3.4'te sözde kodu verilen algoritma çalışır. İkinci aşamada ağda bulunan VLAN'lara düğüm dağıtımını yapan Şekil 3.2'de akış diyagramı, Şekil 3.5'te sözde kodu verilen yük dengeleme algoritması çalışır. Parametrik olarak belirlenen zaman aralıklarında, VLAN ekleme algoritması çağrılır. VLAN'lardan herhangi birinin toplam

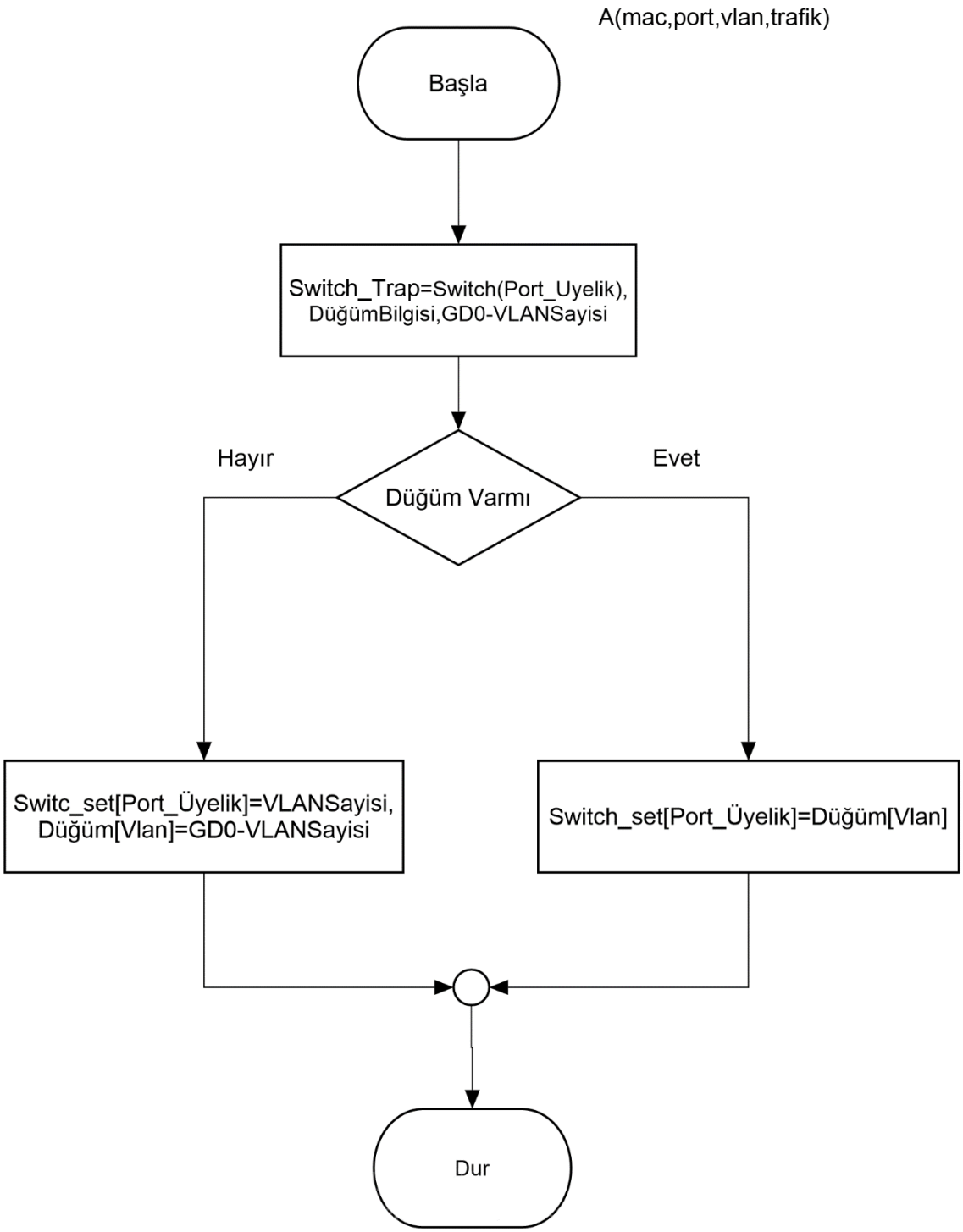
trafiğinin parametrik olarak belirlenmiş olan VLAN toplam trafik eşik değerini aşması durumunda, ağda önceden tanımlanmış, fakat henüz hiçbir üyesi bulunmayan bir VLAN aktif olarak işaretlenir. Aktif VLAN'lar düğüm üyeliği kabul edebilir VLAN'lardır. Belirlenmiş olan eşik değerinin aşılmaması durumunda herhangi bir işlem yapılmaksızın algoritmanın diğer adımlarına devam edilir.



Şekil 3.1. SNMP'ye dayalı dinamik VLAN ekleme algoritması akış diyagramı.



Şekil 3.2. SNMP'ye dayalı dinamik VLAN yük dengeleme algoritması akış diyagramı.



Şekil 3.3. Ağa dahil olan düğümler için üyelik akış diyagramı.

```
//Vlanlar Kontrol ve VlanEkleme Algoritması
//Input: Dizi VLANBilgi[0..n-1,1,1],ilk indis:VLANID;
//ikinci indis: VLAN Toplam Trafik;üçüncü indis
 //VLAN'daki düğüm adedi
//Input:VLAN Trafiği için Eşik Değeri
Start
        if VLANBilgi[0,2] =1
                if VLANBilgi[0,1]<EşikDeğeri
                        goto loop
                else
                        print("Eşik Değerini yükseltin")
                        goto Loop

      else
        if VLANBilgi[0,1]<EşikDeğeri
                        goto Loop
                else
                        VLANBilgi[VLANSayisi+1] ←aktif
                        Algoritma1()//SNMP'ye dayalı dinamik VLAN yük
                                    //dengeleme algoritması

Loop
```

Şekil 3.4. SNMP'ye dayalı dinamik VLAN ekleme algoritması.

```
//Vlanlar Arası Yük Dengeleme Algoritması
//Input: Dizi A[0..n-1,0..3],ilk indis:BilgisayarSayisi
//İkinci indis:(mac,port,vlan,trafik)
//Input:BilgisayarSayisi,VlanSayisi,ToplamTrafik,BilgisayarTrafigi
//Input:Dizi B[0..n],indis:vlansayisi tuttuğu değer trafik toplamı
//Input: Y sistemin başlangıç durumu
Start
if Y=1
        x←0
        for i ←0 to BilgisayarSayisi-1 do
                a[i,2] ←x
                x←x+1
                        if x<VlanSayisi
                                x←0
else
        for i ←0 to BilgisayarSayisi-2 do
                for j ←0 to BilgisayarSayisi-1 do
                        if  a[i,3]<a[j,3]
                                Swap a[i,0] and a[j,0]
                                Swap a[i,1] and a[j,1]
                                Swap a[i,2] and a[j,2]
                                Swap a[i,3] and a[j,3]
        for i ←0 to VlanSayisi-1 do
                a[i,2] ←i
                b[i] ←a[i,3]
        for j←VlanSayisi to BilgisayarSayisi-1 do
                for i←VlanSayisi-1 to 1 step -1 do
                        if b[i]+a[j,3]<=b[i-1]
                                b[i] ←b[i]+a[j,3]
                                a[j,2] ←i
                                break
                        else if i-1=0
                                b[0] ←b[0]+a[j,3]
                                a[j,2] ←0
                                break

Loop
```

Şekil 3.5. SNMP'ye dayalı dinamik VLAN yük dengeleme algoritması.

Şekil 3.5'te sözde kodu verilen algoritmada düğümlerin ürettikleri toplam trafiğe göre, yeni VLAN üyeliklerine karar verme işlemi gerçekleştirilmiştir. Ağdaki anahtar cihazlardan SNMP protokolü vasıtası ile alınan bilgiler bir veritabanında tutulmuş olup karar verme esnasında VLAN'larda hangi düğümlerin en fazla trafiği ürettikleri bilgisi esas alınmıştır. Düğümlerin farklı VLAN'lara üyeliklerinin yapılması ve VLAN sayısı kadar düğüm için bu işlemin gerçekleştirilmesinden sonra geriye kalan düğümler için bu işlemin tekrarlanması ile neticelenir. Örnek olarak 10 tane VLAN bulunan bir ağda 100 tane düğüm var ise bu düğümler ürettikleri trafiğe bakılarak büyükten küçüğe sıralanır. En fazla VLAN sayısı kadar iterasyon gerçekleştirilir (Verilen örnek için en fazla 10 iterasyon). Bir düğümün mevcut VLAN'lardan hangisine üye yapılacağı, düğümün toplam trafiğinin sıradaki VLAN'ın toplam trafiğine eklenerek algoritmada bir sonra gelecek VLAN'ın toplam trafiğinden büyük olup olmama durumuna bakılarak karar verilir. Eğer düğümün üyeliği için kontrol edilen VLAN'ın toplam trafiği kendinden sonra gelen VLAN'ın toplam trafiğinden büyük değilse üyelik işlemi gerçekleştirilir. Aksi halde sonraki VLAN'lar için işlem tekrarlanır. Her değişim sonrasında ağdaki cihazlarda port kapama ve açma işlemi gerçekleştirilir. Bunun sebebi düğümlerin değişen VLAN'larına uygun olarak DHCP sunucusundan yeniden IP almaları gerekmesidir. Bu işlemler sonucunda ilk VLAN'da en büyük, sonrakinde ondan daha az olacak şekilde toplam trafikleri birbirine yakın VLAN'lar oluşur. VLAN'lardaki düğüm sayısı ise düğümlerin ürettikleri trafik değerlerine göre değişiklik arz eder. Örneğin ilk VLAN'da iki tane düğüm olabilirken bir sonrakinde on tane düğüm olabilir. Algoritmaya göre ağın başlangıç veya sistem sıfırlama durumunda olması halinde düğümlerin trafik değerlerinin herhangi bir önemi olmadığından düğümler sırasıyla her VLAN'da düğüm adedi yaklaşık eşit olacak şekilde VLAN'lar arasında paylaştırılır. Örneğin beş adet VLAN'a sahip bir ağda sekiz adet düğüm var ise VLAN'larda sırası ile 2-2-2-1-1 olacak şekilde bir paylaşım gerçekleştirilir.

4. SNMP'YE DAYALI DİNAMİK AĞ TRAFİĞİ DENGELEME ALGORİTMASI PERFORMANS DEĞERLENDİRMESİ

Bu bölümde geliştirilen algoritmanın performans değerlendirmesi için öncelikli olarak fiziksel olarak kurulmuş bir ağdan elde edilen deneysel sonuçlar sunulmuştur. Ardından kurumsal ağlarda sistematik ağ tasarımı için literatürde yer alan yaklaşımlarla VLAN sayısı ve VLAN yayın trafiği maliyetleri açısından karşılaştırma yapılmıştır. Ayrıca literatürdeki dinamik VLAN yaklaşımı içeren çalışmalara karşı avantajları ve dezavantajları değerlendirilmiştir.

Bu karşılaştırmada, önerilen yöntem ile uygulama esnasındaki izlenen yöntemler ve kullanılan teknolojiler arasındaki farklılar sunulmuştur. Tez çalışmasının algoritması literatürde yer alan diğer çalışmaların algoritmalarına benzemediği için, karşılaştırma yapılabilmek amacıyla Bölüm 4.4'te verilen çalışmaların kullandığı parametreler algoritmaya uygulanmış ve sonuçlar sunulmuştur, Bölüm 4.5'te ise belirli kriterler seçilerek karşılaştırma sonuçları bir tablo halinde verilmiştir.

4.1. PERFORMANS DEĞERLENDİRME ORTAMI

Geliştirilen algoritmanın performans değerlendirmesini yapabilmek için farklı senaryolar üretilmiştir. Senaryolarda farklı sayılarda, birbirine bağlı, toplamda üç adet Enterasys marka B5 model Ethernet anahtar, bir adet Extreme marka X440-24t model Ethernet anahtar, Windows işletim sistemine sahip bilgisayarlar ve geliştirilen yazılımın üzerinde çalıştığı yönetim sunucusu kullanılmıştır. Bu yönetim sunucusu aynı zamanda DHCP sunucusu olarak da kullanılmıştır ve VLAN'lara üye olacak düğümlerin IP havuzları bu sunucu üzerinde tanımlanarak dinamik olarak IP adresi almalarına olanak tanınmıştır. Yönetim sunucusu herhangi bir VLAN'a üye değildir. Anahtarlardan biri omurga anahtarı olarak diğerleri ise kenar anahtarlar olarak çalıştırılmıştır. Sistem üzerinde biri varsayılan, on tanesi dinamik, biri güvenlik ve diğeri yönetim VLAN'ı olmak üzere toplamda en fazla 10 adet VLAN test için kullanılmıştır. Ağda en çok 66 adet düğüm kullanılarak trafik gözlemlenmiştir. Ağda düğümlerin kullandığı ortak bir ağ yazıcısı kullanılmış olup bu yazıcının VLAN'ı sabit tutulmuştur. Omurga anahtarda tüm

VLAN'lar arası yönlendirme oluşturulmuştur. Böylece yazıcı tüm VLAN'lardaki düğümler tarafından kullanılabilmiştir.

Bu çalışmanın mevcut ağlara ya da yeni kurulacak olan yerel alan ağlarına uygulanmasında başlıca kabuller şunlardır;

1. Kabul: Ortamda bir Dynamic Host Configuration Protocol (DHCP) sunucusu olmalı ve her VLAN için IP havuzu tanımlanmalıdır.
   - Gerekçe: VLAN'ı farklı her düğümün IP adresi farklı olmalı ve bu IP adresini ortamdaki bir DHCP sunucusundan edinmelidir.
2. Kabul: Ağdaki her uç anahtar üzerinde bütün fiziksel portlar varsayılan VLAN'a üye yapılmalıdır.
   - Gerekçe: Ağa bağlanan her düğüm üzerinde statik IP adresi olmadığında ilk iş olarak ortamda bir DHCP sunucusu arayacaktır. Bu nedenle DHCP sunucusunda bağlı anahtarın önceki VLAN üyeliğine göre IP adresi almaması gerekmektedir.
3. Kabul: Ağdaki her anahtar SNMPv3 protokolünü desteklemelidir.
   - Gerekçe: Ağdaki anahtarların yönetim sunucusu ile olan iletişiminin güvenli ve kimlik doğrulama yönteminin kullanılması gerekmektedir.
4. Kabul: Ağda köprü anahtarlar üzerinde VLAN'lar etiketli olarak taşınabilmelidir.
   - Gerekçe: Ağ yapısı büyük olduğunda ağlarda VLAN'lar birden çok anahtar atlayabilir ve bir paketin hangi VLAN'a üye olduğu bilgisi anahtarlar arasında taşınması zorunludur.
5. Kabul: Güvenlik düzeyleri farklı olan VLAN'lara üye yapılacak düğümler için düğümlerin fiziksel adresleri veritabanında tanımlanmalıdır.
   - Gerekçe: Güvenlik düzeyleri farklı olduğu VLAN'larda düğümler her zaman aynı VLAN'a üye olmak zorundadırlar, bu tip düğümler için ürettikleri trafik değerlerine göre dinamiklik söz konusu değildir. Bu nedenle güvenlik düzeyi farklı her düğümün önceden MAC adresi bilinmek ve VLAN'ı ayarlanmak zorundadır.
6. Kabul: Ağ kaç VLAN'a bölünmek isteniyorsa (Özel güvenlik düzeyine sahip olanlar da dahil) o kadar VLAN omurga anahtar üzerinde tanımlanmalıdır.
   - Gerekçe: SNMP ile omurga anahtar üzerinde yönlendirmeler için komut bulunmamaktadır. Bu nedenle yönlendirme yapılması istenen VLAN'lar omurga anahtar üzerinde tanımlı olmak zorundadır.

7. Kabul: Ağda kullanılacak VLAN'lar algoritma doğrultusunda geliştirilen yazılımda da tanımlanmalıdır.
    - Gerekçe: Yazılım ağda kullanılmaya başlandığı andan itibaren kaç adet VLAN ve hangi VLAN'lar dinamik hangi VLAN'lar özel güvenlik düzeyine sahip olduğu tanımlanmak zorundadır.
8. Kabul: MAC adresi bilinmeyen bütün düğümler VLAN'ı değiştirilebilir düğüm olarak kabul görmelidir.
    - Gerekçe: MAC adresi bilinmeyen düğümlerin özel güvenlik düzeyine sahip bir şekilde ağa erişmesine gerek olmadığı için algoritma her çalıştığında sonuç olarak ne çıktı üretiliyorsa, düğüm farklı farklı VLAN'lara üye olabilir.
9. Kabul: Anahtar cihazlarda statik IP yapılandırmasının önüne geçilmesi için DHCP Snooping denilen özellik aktif edilmelidir.
    - Gerekçe: Düğümler elle verilmiş statik IP yapılandırmalarına sahip olurlarsa ağa erişmeleri ve internete çıkmaları mümkün olmayacaktır.

Ağdaki tüm anahtarların güvenlik ilkeleri gereği SNMPv3 protokolünü desteklemeleri gerekmektedir. Düğümlerin IP adres yapılandırmaları ise otomatik olduğu için yönetim sunucusunun üzerinde bulunan DHCP hizmeti vasıtasıyla VLAN'lara atanacak adres havuzları ayarlanmış ve sorunsuz bir şekilde IP adresi almaları sağlanmıştır.

Geliştirilen yazılımda SNMP'nin get, set ve trap mekanizmaları kullanılarak kenar anahtarlardan bilgiler belirli sürelerde alınıp dinamik VLAN atamasına karar vermek amacıyla kullanılmıştır. Yazılımda kullanılan başlıca oid'ler ise şunlardır;

1. 1.3.6.1.2.1.31.1.1.1.5.x: Bir portun çıkış yönündeki trafiği.
2. 1.3.6.1.2.1.31.1.1.1.3.x: Bir portun giriş yönündeki trafiği.
3. 1.3.6.1.2.1.17.7.1.4.3.1.x: Bir VLAN oluşturup porta atama.
4. 1.3.6.1.2.1.17.7.1.4.x: Hangi Portun hangi VLAN'a üye olduğu.
5. 1.3.6.1.2.1.4.22.1.x: MAC adresi ve IP adresi sorgulama.
6. 1.3.6.1.2.1.2.2.1.x: Port açıp kapatma.
7. 1.3.6.1.2.1.4.34.1.x: VLAN arayüze IP adresi atama.

4.2. ALGORİTMA ÇALIŞMA SÜRESİ

Kişisel bilgisayarlar ağ kartı üzerinden ağ ortamına bağlandıklarında, şayet statik bir IP yapılandırmasına sahip değillerse, ortamda bir DHCP sunucusu ararlar. DHCP sunucusu ile aralarında belirli protokoller ile IP yapılandırmasına sahip olurlar. Bir düğüm ağa bağlı olduğu anahtarın portu her açılıp kapandığı zaman DHCP sunucusundan IP alma işlemi tekrarlanır.

Ağ yöneticileri ağda statik IP tanımlı bilgisayarların ağa erişimini kısıtlayabilirler. Bu özelliğin kullanılabilmesi için anahtarlarda DHCP Snooping özelliğinin port bazlı aktif edilmesi gerekir. Bunun sebebi düğümlerin kendi hakları çerçevesinde ağa ve internete erişmelerini sağlamaktır. Bu özellik aktif edilmese bile ağda bir güvenlik zafiyeti oluşmaz ancak IP çakışmaları gözlemlenebilir.

Algoritmanın çalışma süresinin ölçülmesine gerek duyulmamıştır. Çünkü hiçbir düğümün algoritma çalışma esnasında ağ ile bağlantıları koparılmaz. Sadece algoritma sonucuna göre düğümün anahtarda bağlı bulunduğu portun yeni VLAN üyeliği yapılarak anlık olarak kapatılıp açılır. Bu sayede şayet düğüm ağa bağlı ise bağlı bulunduğu portun yeni VLAN üyeliğine göre yeni IP adresi alması ya da eski üyeliğine göre eski IP adresi ile devam etmesi sağlanmış olur.

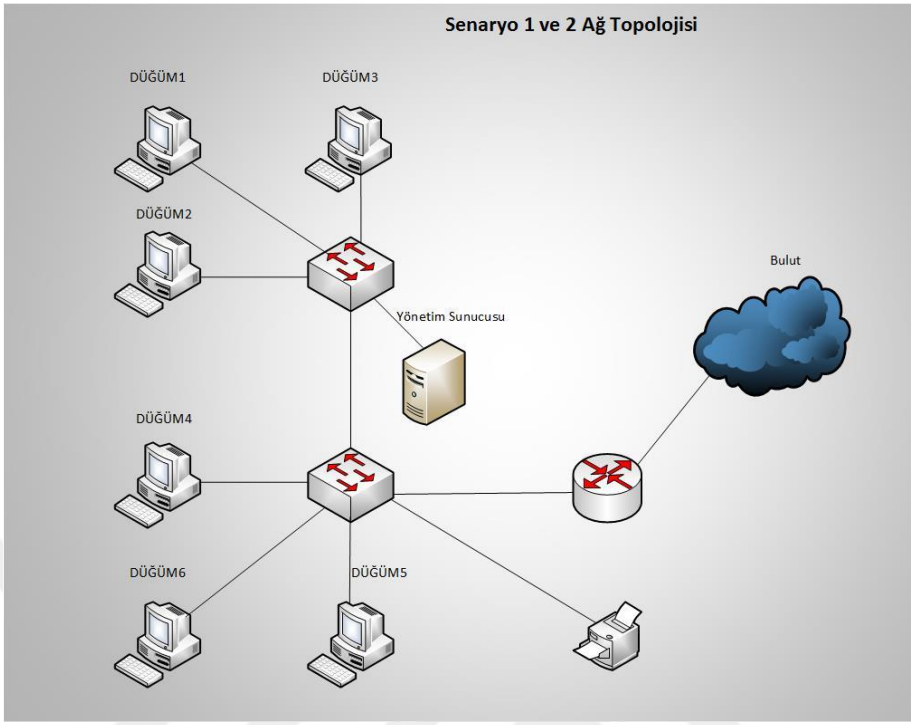
4.3. UYGULANAN SENARYOLAR

Geliştirilen algoritma beş farklı senaryo oluşturularak test edilmiştir. Senaryolar ve elde edilen bulgular aşağıda verilmiştir.

Senaryo 1: Sistem başlangıç veya reset durumu: Başlangıçta veri trafiğinin hiç olmadığı durumda 2 anahtar, 3 adet VLAN, 6 adet düğüm ve bir adet yönetim sunucusunun bulunduğu Şekil 4.1’de verilen ağ topolojisi oluşturulmuştur. Algoritmanın çalışması sonucunda;

1. Her bir VLAN’da eşit sayıda düğüm olacak şekilde dağıtılmıştır.
2. Algoritmanın çalıştırılması sonucu Çizelge 4.1’de verilen üyelikler gerçekleşmiştir.
3. Düğüm sayısı VLAN sayısının tam katı olmadığı durumlarda artan tek düğüm ilk VLAN’a üye yapılır.

4. Bu senaryo sistem başlangıç durumu ve sistemin yeniden başlatılması durumu ile aynıdır.



Şekil 4.1. Başlangıç ve reset durumu VLAN üyelikleri.

Çizelge 4.1. Başlangıç ve reset durumu VLAN üyelikleri

	VLAN1	VLAN2	VLAN3
DÜĞÜM1	✓		
DÜĞÜM2	✓		
DÜĞÜM3		✓	
DÜĞÜM4		✓	
DÜĞÜM5			✓
DÜĞÜM6			✓

Senaryo 2: Senaryo 2, Senaryo1'in ağ topolojisi kullanılarak gerçekleştirilmiş fakat farklı bir durum değerlendirilmiştir. Her bir düğüm üzerine kurulmuş olan 3. Parti Ostinato ağ trafik üreticisi kullanılarak [53] Şekil 4.1'de verilen ağ topolojisinde düğümlere yaklaşık olarak DÜĞÜM1:148KB, DÜĞÜM2:3558KB, DÜĞÜM3:445KB, DÜĞÜM4:296KB,

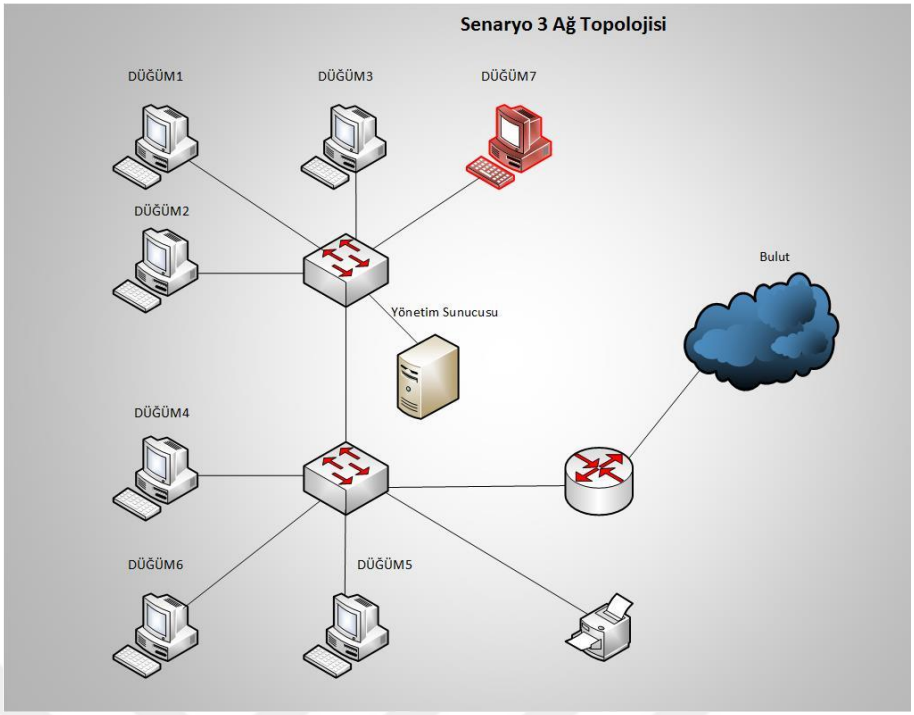
DÜĞÜM5:1779KB, DÜĞÜM6:741KB olacak şekilde trafikler ürettirilmiştir. Trafikler ürettirildikten sonra algoritmanın ağ kontrol mekanizması çalıştırılmıştır. Bu kontrol sonrasında öncelikle ağ trafik değerlerine göre büyükten küçüğe doğru sıralama yapılmış daha sonra her bir düğüm sırasıyla VLAN'lara paylaştırılarak belli bir döngü ve kontrol mekanizması içinde trafiklerin birbirine yakın olacağı şekilde üyeliklerin dağıtıldığı gözlemlenmiştir.

Algoritmanın çalışması sonucunda Çizelge 4.2'de verilen düğümler ve VLAN üyelikleri oluşmuştur. VLAN trafikleri Vlan1:3558KB (DÜĞÜM2); Vlan2:1779KB (DÜĞÜM5); Vlan3:1631KB (DÜĞÜM1 + DÜĞÜM3 + DÜĞÜM4 + DÜĞÜM6) olarak gerçekleşmiştir.

Çizelge 4.2. Senaryo 2'de algoritma sonucu VLAN üyelikleri.

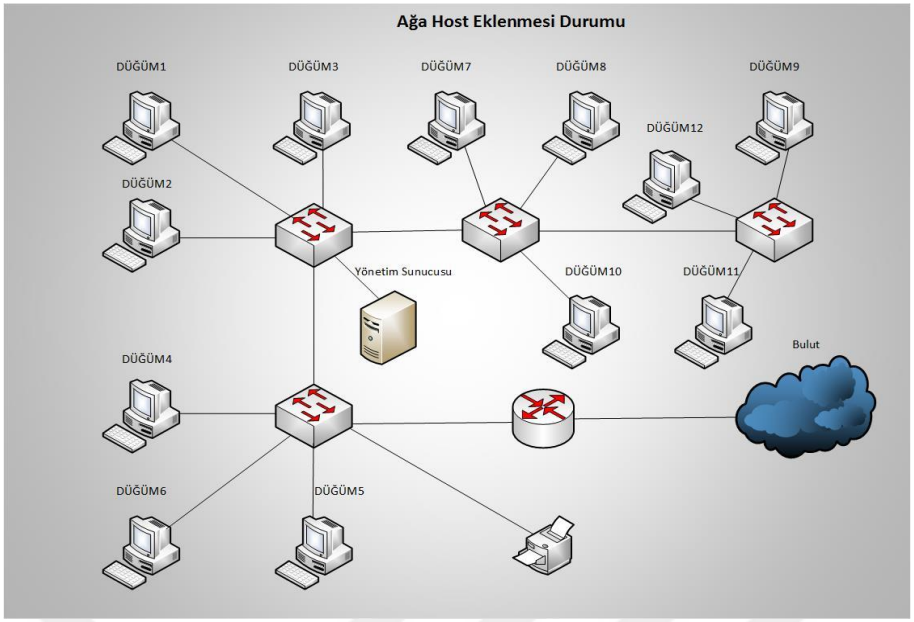
	VLAN1	VLAN2	VLAN3
DÜĞÜM1			✓
DÜĞÜM2	✓		
DÜĞÜM3			✓
DÜĞÜM4			✓
DÜĞÜM5		✓	
DÜĞÜM6			✓

Senaryo 3: Şekil 4.2'de verilen ağ topolojisine göre ağa özel güvenlik düzeyine sahip bir düğümün dahil olması durumu: Ağ 6 adet düğüm, 1 adet Yönetim Sunucusu, 2 adet anahtar, 3 VLAN ve 1 adet özel güvenlik düzeyli VLAN kullanılarak oluşturulmuştur. Özel güvenlik düzeyine sahip VLAN'lar ağ yöneticileri, sistem yöneticileri ve gerekli görülen kullanıcılar için farklı güvenlik düzeylerinde tanımlanabilmektedir. Veritabanında yer alan DÜĞÜM7, algoritma tarafından MAC adresi bilgisi kullanılarak özel güvenlik düzeyli VLAN'a üye yapılmıştır.



Şekil 4.2. Güvenli VLAN senaryosu topolojisi.

Senaryo 4: Bu senaryoda Şekil 4.3'teki gibi fiziksel olarak konumlandırılmış ve Ostinato yazılımı ile ürettirilmiş Çizelge 4.3'teki trafik yüklerine sahip 10 adet düğüm içeren, güvenlik düzeyleri eşit üç VLAN bulunan ağa 16 KB trafiğe sahip iki yeni düğüm eklenmesi durumu gerçekleştirilmiştir. Düğümlerin Çizelge 4.3'te verilen trafik yükünü üretmelerinin ardından, algoritma tarafından Şekil 4.5'te gösterildiği gibi 3 adet VLAN'a dağıtımı yapılmıştır. Ağa yeni eklenen düğümlerden birinin VLAN2'ye diğerinin VLAN3'e üyeliği algoritma tarafından gerçekleştirilmiştir. Dinamik dağıtım sonunda Şekil 4.5'te verilen toplam VLAN trafikleri elde edilmiştir.



Şekil 4.3. Ağa düğüm eklenmesi durumu.

Çizelge 4.3. Düğümler tarafından üretilen trafik değerleri.

	Ürettiği Toplam Trafik(KB)
DÜĞÜM1	120
DÜĞÜM2	51
DÜĞÜM3	158
DÜĞÜM4	197
DÜĞÜM5	185
DÜĞÜM6	174
DÜĞÜM7	106
DÜĞÜM8	120
DÜĞÜM9	102
DÜĞÜM10	152

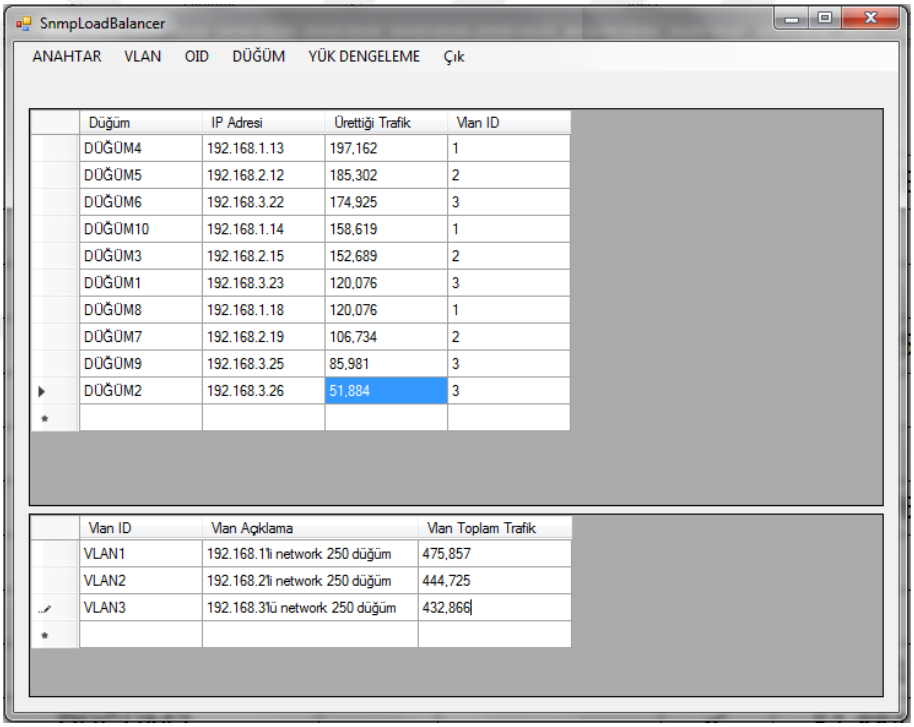
DÜĞÜM1-DÜĞÜM10'a ait üretilen trafik miktarları Çizelge 4.3'te verilmiştir. Ağa ilk

VLAN belirleme işleminden sonra Çizelge 4.4'te ürettikleri trafik değerleri gösterilen DÜĞÜM11 ve DÜĞÜM12 dahil edilmiştir.

Çizelge 4.4. Ağa sonradan dahil olan düğümler ve trafikleri.

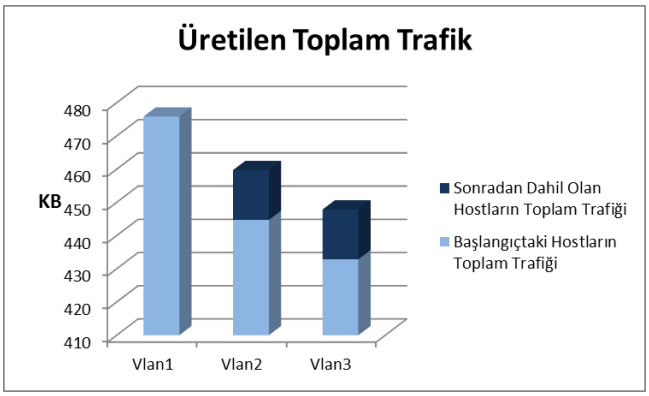
	Ürettiği Toplam Trafik(KB)
DÜĞÜM11	16
DÜĞÜM12	16

Çizelge 4.4'te DÜĞÜM11 ve DÜĞÜM12'nin ürettikleri trafik gösterilmiş olup, bu iki düğümün ağa katılmasından önce algoritmanın çalışması sonucunda ağa ilk dahil olan Düğüm1-Düğüm10 aralığındaki düğümlerin üyelikleri Şekil 4.4'te verilmiştir.



Şekil 4.4. Senaryo 4 başlangıç düğümlerinin VLAN'lara dağılımı.

Algoritmaya göre ağa sırasıyla dahil olan DÜĞÜM11'in VLAN2'ye, DÜĞÜM12'nin VLAN3'e üyelikleri yapılmıştır. Şekil 4.5'te senaryonun birinci aşamasında dahil olan düğümlerin ve ikinci aşamasında dahil olan düğümlerin oluşturduğu trafiğin VLAN'lara göre dağılımı verilmiştir.



Şekil 4.5. Senaryo 4 tüm düğümlerin oluşturduğu trafiğin VLAN'lara dağılımı.

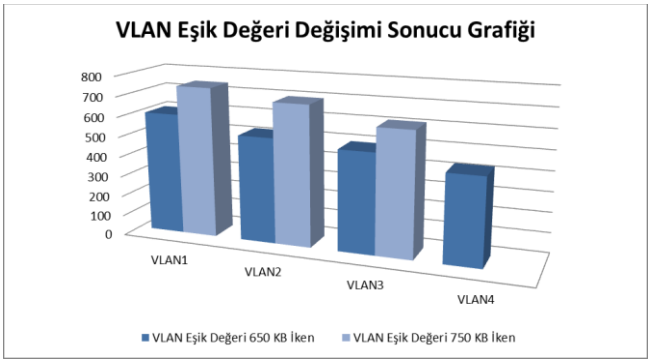
Şekil 4.5'te verilen değerlerden anlaşılacağı üzere ağdaki tüm düğümlerin VLAN'lara dağılımı sonrasında her üç VLAN birbirlerine yakın trafik değerlerine ulaşmıştır.

Senaryo 5: Bu senaryoda, Senaryo 4 için oluşturulmuş ağ topolojisi kullanılmış fakat farklı bir durum olan VLAN eşik değerinin nasıl bir sonuç ortaya koyduğu gözlemlenmiştir. Bu senaryo için Çizelge 4.5'te verilen düğüm trafikleri ürettirilmiştir.

Çizelge 4.5. Senaryo 5, VLAN ekleme algoritması için düğüm trafikleri.

	Ürettiği Toplam Trafik(KB)
DÜĞÜM1	171
DÜĞÜM2	102
DÜĞÜM3	209
DÜĞÜM4	248
DÜĞÜM5	236
DÜĞÜM6	225
DÜĞÜM7	157
DÜĞÜM8	171
DÜĞÜM9	153
DÜĞÜM10	203
DÜĞÜM11	67
DÜĞÜM12	118

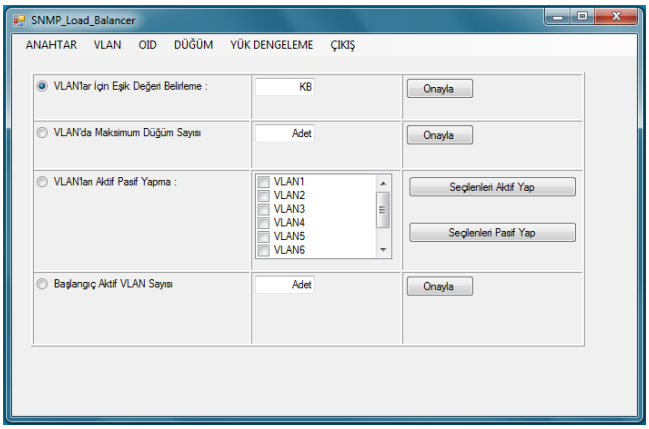
Başlangıçta VLAN eşik değeri 750 KB olarak belirlenmiş senaryonun başlangıcında belirtilen ve Şekil 4.6'da gösterilen dağılım sonucu elde edilmiştir. VLAN eşik değerini 650 KB'a çektiğimiz zaman ağımızda VLAN 4 aktif olarak kullanılmaya başlanmış olup ve Şekil 4.6'da gösterilen VLAN dağılımı elde edilmiştir.



Şekil 4.6. VLAN eşik değeri değişimi sonucu VLAN trafik dağılımları.

Şekil 4.6'da başlangıçta 750 KB olarak belirlenen eşik değeri bir sonraki aşamada trafikler aynı tutularak 650 KB'a çekilmiştir. Bunun sonucunda algoritma VLAN 4'ü aktif hale getirmiş ve düğümlerin üyelikleri değişerek VLAN dağılımları sonucu eşik değerini geçmeyen VLAN trafikleri oluştuğu gözlemlenmiştir.

Senaryo 5 için kullandığımız ve algoritmamız doğrultusunda geliştirilmiş yazılım arayüzü Şekil 4.7'de verilmiştir.



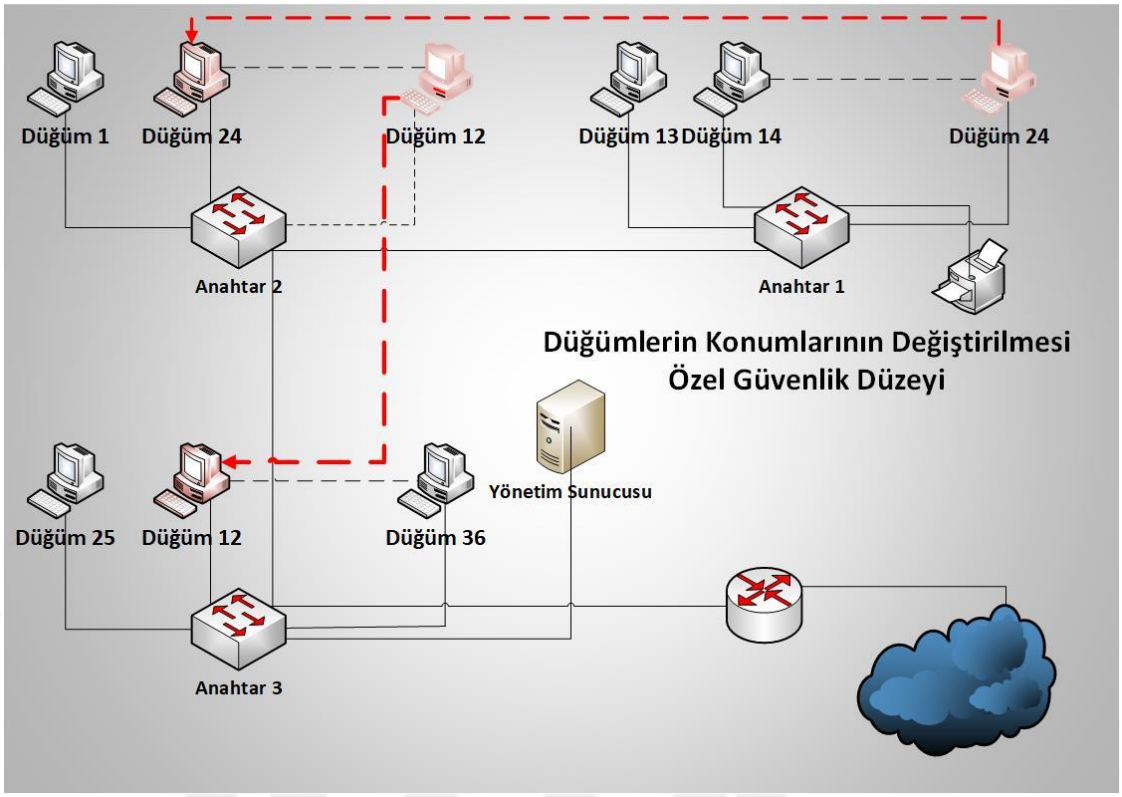
Şekil 4.7. VLAN'lar için eşik değerinin belirlenebileceği yazılım arayüzü.

Şekil 4.7'de yazılımın ağda bulunan VLAN'lar için temel bazı ayarlar yapabileceğimiz görülmektedir. Bu ayarlar sonrasında sistem, düğümlerin VLAN'lar arasında dağılımını tekrardan otomatik olarak yapmaktadır. Böylelikle yapılan her değişiklik o esnada gerçek zamanlı olarak ağa uygulanmaktadır.

Senaryo 6: Bu senaryoda özel güvenlik düzeyine sahip iki düğümün ağda fiziksel olarak yer değiştirmesi sağlanmıştır. Şekil 4.8'de gösterilen ağ topolojisi kullanılmıştır. *Düğüm 12* ve *Düğüm 24* ağda fiziksel olarak farklı anahtarların farklı portlarına taşınmıştır.

Düğüm 12 özel güvenlik düzeyli VLAN 10 *Düğüm 24* ise özel güvenlik düzeyli VLAN 11'e üyedir. *Düğüm 12* ağda 2. anahtar üzerinde 22. portunda ağa bağlı iken, 3. anahtarın 2. portuna taşınmış, *Düğüm 24* ise 1. anahtarın 23 numaralı portundan, 2. anahtarın 2. portuna taşınmıştır.

Bu fiziksel taşıma sonucu anahtarlar *Düğüm 12* ve *Düğüm 24*'ün veri tabanındaki üyeliklerine göre Çizelge 4.6'da gösterildiği üzere tekrar yapılandırılmıştır. Burada dikkat edilmesi gereken husus her anahtar üzerinde varsayılan VLAN olarak yönetim sunucusunun da bağlı olduğu portun üye olduğu yönetim VLAN'ının tanımlı olması gerekliliğidir. Bu gereklilik portlara bir düğümün bağlandığında belirli bilgilerinin yönetim sunucusuna iletiliyor olmasından doğmaktadır. Bu durum yazılımın portun hangi VLAN'a üye olması gerektiğine karar verene kadar kısa bir süre devam eder. Daha sonra yönetim sunucusu o düğüm için uygun konfigürasyonu anahtara yollar ve port kapatılıp açılır. Portun kapatılıp açılması ise yönetim sunucusu üzerinden üye olduğu VLAN'a ait DHCP havuzundan IP kiralanması için gereklidir. IP atama işlemi Özel güvenlik düzeyine sahip VLAN'a üye düğümler için DHCP'de önceden VLAN'lar için oluşturulmuş rezerve IP adresleri veya IP blokları ile gerçekleştirilir.



Şekil 4.8. Özel güvenlik düzeyine sahip düğümün yer değiştirmesi.

Çizelge 4.6. Özel güvenlik düzeyi konum değişimi.

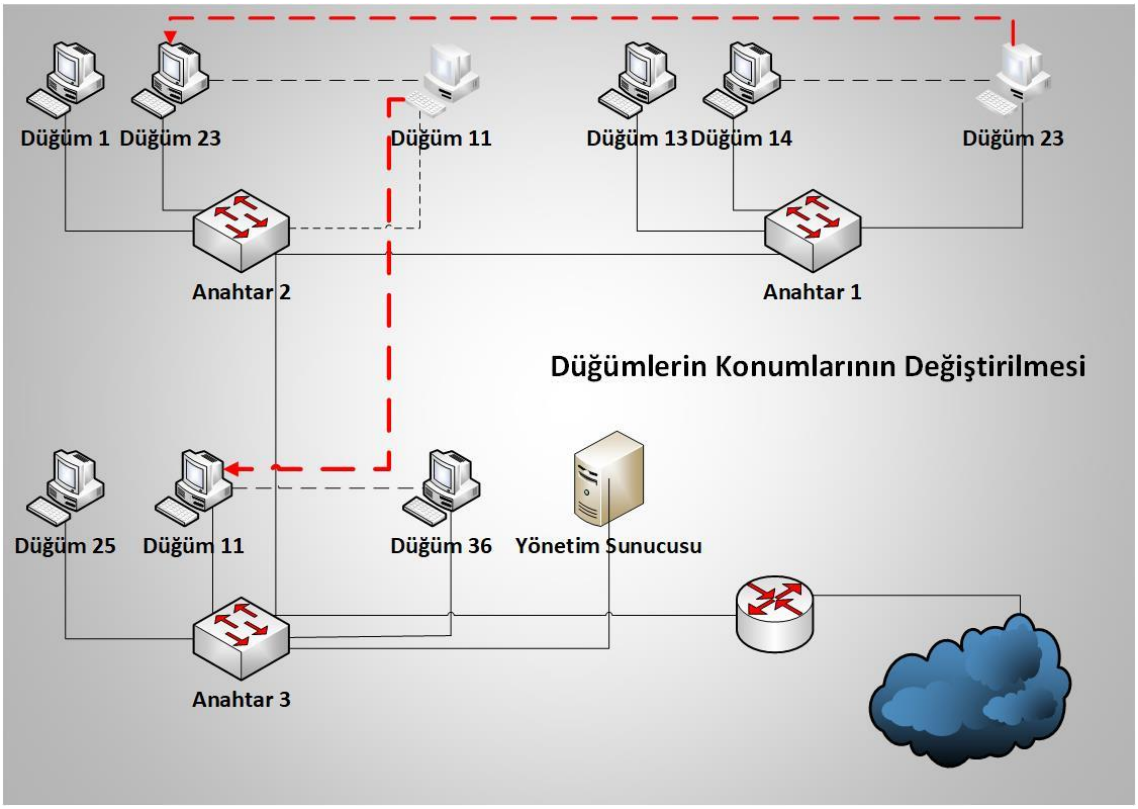
	Önceki Üyelik Durumu	Sonraki Üyelik Durumu
Anahtar 1-Port 23	VLAN 11	Yönetim VLAN'ı
Anahtar 2-Port 2	Yönetim VLAN'ı	VLAN 11
Anahtar 2-Port 22	VLAN 10	Yönetim VLAN'ı
Anahtar 3-Port 2	Yönetim VLAN'ı	VLAN 10

Çizelge 4.6'da Senaryoda kullanılan anahtarların ilgili Portlarının VLAN üyeliklerinin değişimleri detaylı olarak verilmiştir. Ayrıca ağda sadece özel güvenlik düzeyi VLAN 11'e üye düğümlerin ulaşabileceği bir yazıcı kullanılmış ve fiziksel olarak yer değişme sonucu bu erişimin kısıtlanmadığı gözlemlenmiştir.

Senaryo 7: Bu senaryoda Şekil 4.9'da gösterilen ağ topolojisi kullanılmış olup Senaryo 6'dan farklı olarak düğümler *özel güvenlik* düzeyli bir VLAN'a değil normal güvenlik düzeyine sahip VLAN'lara üyedirler. Bu senaryoda toplam 5 adet VLAN ve 36 adet düğüm kullanılmıştır.

Bu senaryoda düğümler her ne kadar yer değiştirilme esnasında ağdan belirli bir süre koparılmış olsa da algoritmanın karar verme zaman aralığından önce veya sonra ağa geri dönmüş olmaları çok önemlidir. Karar verme algoritması sözde kodu Şekil 3.5'te verilmiştir.

Düğümler bu senaryoda karar verme algoritmasından önce yer değiştirmiş olsalardı Senaryo 6'da gösterilmiş olduğu gibi eski bulundukları VLAN'a üye olmuş olacaklardı. Ancak ağdan belirli bir süre koparıldıkları ve karar verme algoritması çağrıldıktan sonra ağa geri dahil edildikleri için ürettikleri trafik miktarı diğer düğümlere nazaran az olduğu için Çizelge 4.7'de gösterildiği gibi aynı ve indis numarası en düşük VLAN'a üye olmuşlardır.



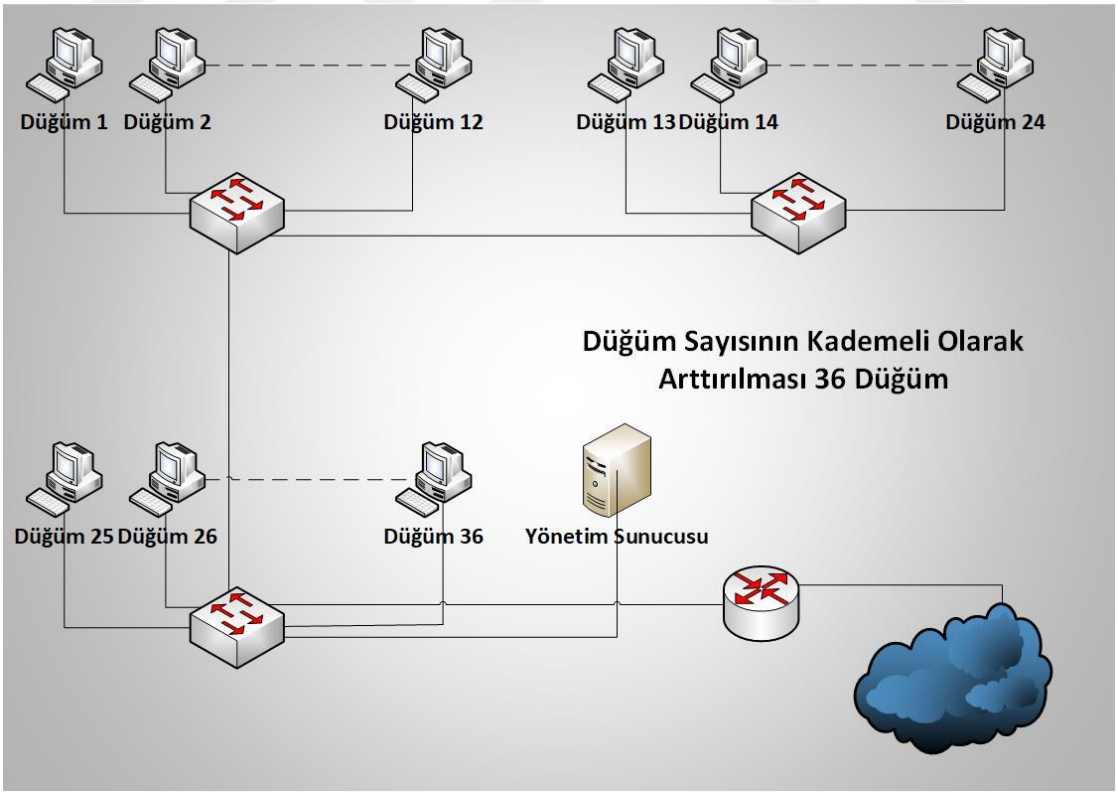
Şekil 4.9. Normal düğüm ağda yer değiştirmesi.

Çizelge 4.7. Düğümlerin fiziksel olarak konum değiştirilmesi.

	Önceki VLAN üyeliği	Ağdan Koparılma Süresi	Sonraki VLAN üyeliği
Düğüm 11	VLAN 2 (Anahtar 2-Port 11)	3 saat	VLAN 5 (Anahtar 3-Port 4)
Düğüm 23	VLAN 3 (Anahtar 1-Port 11)	4 saat	VLAN 5 (Anahtar 2-Port 11)

Senaryo 8: Bu senaryo için Şekil 4.10'da gösterilen ağ topolojisi kullanılmıştır. Bu senaryoda karar verme algoritması sonrası ağa yeni düğümler dahil edilmiştir. Başlangıçta 18 düğümden oluşan ağ sonrasında 18 düğüm daha eklenmiştir. Senaryo 6 adet VLAN ile gerçekleştirilmiş olup sonradan eklenmiş 18 adet düğüm için trafikler ürettirildikten sonra karar verme algoritması çağrılmıştır. Karar verme algoritmasının 2. çağrılması sonucu hiçbir VLAN'ın toplam trafiği VLAN eşik değerini aşmadığı için VLAN sayısı 6 olarak değişmemiştir. Ağa sonradan dahil edilen düğümler için Bölüm 3-Şekil 3.3'de verilen akış diyagramı doğrultusunda VLAN üyeliklerine karar verilir. Bu senaryoda düğümler ağda ilk defa bulundukları için ilk bağlandıklarında herbirinin VLAN'ı indisi en büyük olan 6 olarak ayarlanmıştır. Ağa bağlandıktan sonra ürettikleri trafik değerleri ve yük dengeleme yani VLAN karar verme algoritması ilk çalışmasından sonraki VLAN üyelikleri Çizelge 4.8'de verilmiştir.

Yukarıdaki akış diyagramına göre bir düğüm şayet ağda daha önce bulunmuş ise, veri tabanından hangi VLAN'a üye olduğuna dair bilgiye ulaşılarak ağa bağlandığı anahtarın bağlı olduğu portuna o üyelik bilgisi ayarlanır. Düğüm ağda ilk defa bulunuyorsa ağda her zaman en az toplam trafik değerine sahip olacak olan en büyük indisli VLAN'a üye yapılır. Bu üyelik bir dahaki yük dengeleme algoritması çağırılıncaya kadar aynı kalır



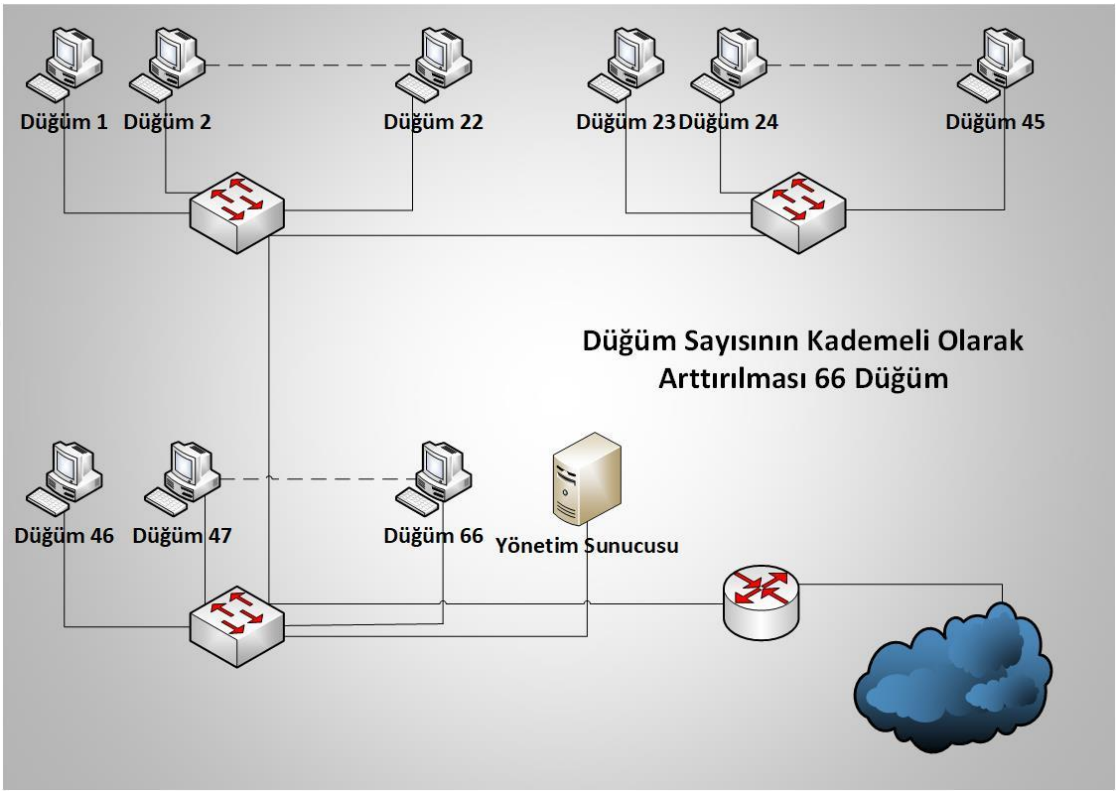
Şekil 4.10. Ağdaki düğüm sayısının arttırılması.

Çizelge 4.8. Ağdaki düğüm sayısının 36'ya çıkarılması.

	İlk VLAN Üyeliği	Ürettiği Toplam Trafik (KB)	Son VLAN Üyeliği
DÜĞÜM 19	VLAN6	599538	VLAN1
DÜĞÜM 20	VLAN6	349499	VLAN3
DÜĞÜM 21	VLAN6	582096	VLAN2
DÜĞÜM 22	VLAN6	657262	VLAN6
DÜĞÜM 23	VLAN6	233618	VLAN6
DÜĞÜM 24	VLAN6	667385	VLAN4
DÜĞÜM 25	VLAN6	688683	VLAN2
DÜĞÜM 26	VLAN6	573510	VLAN3
DÜĞÜM 27	VLAN6	353261	VLAN2
DÜĞÜM 28	VLAN6	552048	VLAN6
DÜĞÜM 29	VLAN6	339354	VLAN4
DÜĞÜM 30	VLAN6	558479	VLAN5
DÜĞÜM 31	VLAN6	248930	VLAN5
DÜĞÜM 32	VLAN6	431386	VLAN1
DÜĞÜM 33	VLAN6	561858	VLAN4
DÜĞÜM 34	VLAN6	664366	VLAN5
DÜĞÜM 35	VLAN6	677529	VLAN3
DÜĞÜM 36	VLAN6	741196	VLAN1

Senaryo 9: Bu senaryo için Şekil 4.11’de gösterilen ağ topolojisi oluşturulmuştur. Senaryo 8’den farklı olarak, ağda bulunan 3 anahtarın da uplink diye tabir ettiğimiz birbirlerine ve ağa bağlanma portları hariç diğer bütün portlarına birer düğüm gelecek şekilde tasarlanarak oluşturulmuştur. Düğümlere belirli bir süre trafik ürettirildikten sonra VLAN eşik değerinin aşıldığı ve yeni bir VLAN’nın aktif edilerek bu VLAN’a da

düğümlerin üye olduğu gözlemlenmiştir. Başlangıçta 6 adet VLAN ile başlanan senaryoda ilk yük dengeleme algoritması çağrılma aşamasından sonra 7. VLAN diğer VLAN'lardan en büyüğü olan VLAN1'in belirlediğimiz VLAN eşik değerinin aşılmasıyla birlikte aktif olarak kullanıma açılmıştır. Bu işlemlerden sonra VLAN'ların toplam trafikleri ve üye düğüm sayıları Çizelge 4.9'da detaylı olarak verilmiştir.



Şekil 4.11. Ağdaki düğüm sayısının arttırılması.

Çizelge 4.9. Düğüm sayısısın maksimum yapılması.

	Düğüm Sayısı	Toplam Trafik (KB)
VLAN1	10	3645677
VLAN2	10	3467623
VLAN3	10	3364860
VLAN4	9	3138770
VLAN5	9	3086880
VLAN6	9	3029769
VLAN7	9	2944848

Senaryo 10: Bu Senaryoda Senaryo 9'daki ağ topolojisi kullanılarak ağdaki düğümlere daha fazla trafik ürettirilerek ağın durumu gözlemlenmiştir. 10 adet VLAN kullanılmış ve 15 düğüme diğer düğümlerden daha fazla trafik ürettirilmiştir. Yük dengeleme algoritması çalıştırıldıktan sonra düğümlerin VLAN'lara dağılımı ve VLAN'ların toplam trafikleri Çizelge 4.10'da detaylı olarak verilmiştir.

Çizelge 4.10. Toplam trafiğin arttırılması.

	Düğüm Sayısı	Toplam Trafik (KB)
VLAN1	7	2.965
VLAN2	7	2.894
VLAN3	7	2.839
VLAN4	7	2.789
VLAN5	7	2.767
VLAN6	7	2.578
VLAN7	6	2.421
VLAN8	6	2.351
VLAN9	6	2.274
VLAN10	6	2.206

4.4. KURUMSAL AĞ SİSTEMATİK YAKLAŞIMLARI İLE KARŞILAŞTIRMA

Bölüm 1.5'te bahsedilmiş olan çalışmalardan biri olan Yu-Wei (Eric) Sung ve arkadaşlarının "Towards Systematic Design of Enterprise Networks" [4] isimli çalışmalarında, kurumsal ağlarda düğümlerin ürettikleri veri trafiği ve broadcast trafiklerinin tahmini değerlerine göre ağın yapılandırılmasına yönelik ağ yöneticilerine tavsiyelerde bulunmak mahiyetinde bir algoritma geliştirmişlerdir.

Bu algoritma belirli bazı kriterlere göre ağda kaç VLAN olması gerektiği ve hangi

düğümlerin hangi VLAN'lara üye olacaklarını belirlemektedir.

Sistematik ağ tasarımı için kullanılan kriterlerden biri vlan sayısı, diğeri broadcast maliyetidir. Yu-Wei Eric Sung broadcast maliyetini aşağıda verilen Denklem (4.1)'deki şekilde hesaplamışlardır [4].

$$\mathrm{Br}(V_i, S_k) = N_i \times B_i \times W_{ik} \tag{4.1}$$

Bu denklemde V_i i'inci vlan, $B_r(V_i,S_k)$ broadcast maliyeti, spanning tree protokolü kullanılan ağda S_k 'nın root bridge olarak seçilmesi durumunda W_{ik} anahtarlar arasındaki bağlantı sayısı, N_i ise i'inci VLAN'daki düğüm sayısı, B_i i'inci VLAN'daki düğümlerin ürettiği ortalama broadcast trafiğini temsil etmektedir.

Yine aynı çalışmada VLAN adedinin ağa getireceği maliyet Denklem (4.2) ile minimize edilmiştir.

$$\min(\ C(x) + \max\{B_r(V_i), 1 \leq i \leq x\}) \tag{4.2}$$

Burada $B_r(V_i)$ spanning tree protokolünde optimum root bridge seçilmesi durumundaki broadcast maliyetini temsil etmektedir. *C(x)* ise, *x* adet VLAN'a sahip olma maliyetidir ve Denklem (4.3) ile karar verilir.

$$C(x) = \begin{cases} 0, eğer\ x \leq maksimum_vlan_sayısı \\ \infty\ eğer\ x > maksimum_vlan_sayısı \end{cases} \tag{4.3}$$

Burada maksimum_vlan_sayısı, anahtarlar üzerinde tanımlanabilecek en büyük VLAN adedini belirtmektedir.

Bu çalışma 200 yönlendirici ve 1300 anahtarlı 182 VLAN aktif olarak toplamda 15084 düğümle, her bir düğümün Ostinato üreteci ile rasgele trafik üretmeleri sağlanarak test edilmiştir.

Performans değerlendirmesi yapmak için [4]'teki ağ parametreleri kullanılmıştır. Bu parametreler Çizelge 4.11'de verilmiştir.

Çizelge 4.11. Karşılaştırma için kullanılan ağ parametreleri.

Performans Değerlendirme Parametreleri	
Düğüm Sayısı	15084

Çizelge 4.11. (devam). Karşılaştırma için kullanılan ağ parametreleri.

Performans Değerlendirme Parametreleri	
Anahtar Sayısı	1300
VLAN Sayısı	182
VLAN Başına Düşen Ortalama Düğüm Sayısı	82,9
Düğüm Başına Üretilen Ortalama Broadcast Trafiği	0.004 paket/saniye
Düğüm Başına Üretilen Maksimum Broadcast Trafiği	2.12 paket/saniye
Gözlem Süresi	24 Saat.

Devam eden kısımlarda performans değerlendirmeleri yapılırken Yu-Wei Eric Sung ve arkadaşları tarafından önerilen yaklaşım "sistematik", ağ yöneticilerinin manuel olarak yaptıkları tasarım "geleneksel" ve önerdiğimiz sistematik yaklaşım için de "*VLAN_BTYD*" olarak kullanılmıştır.

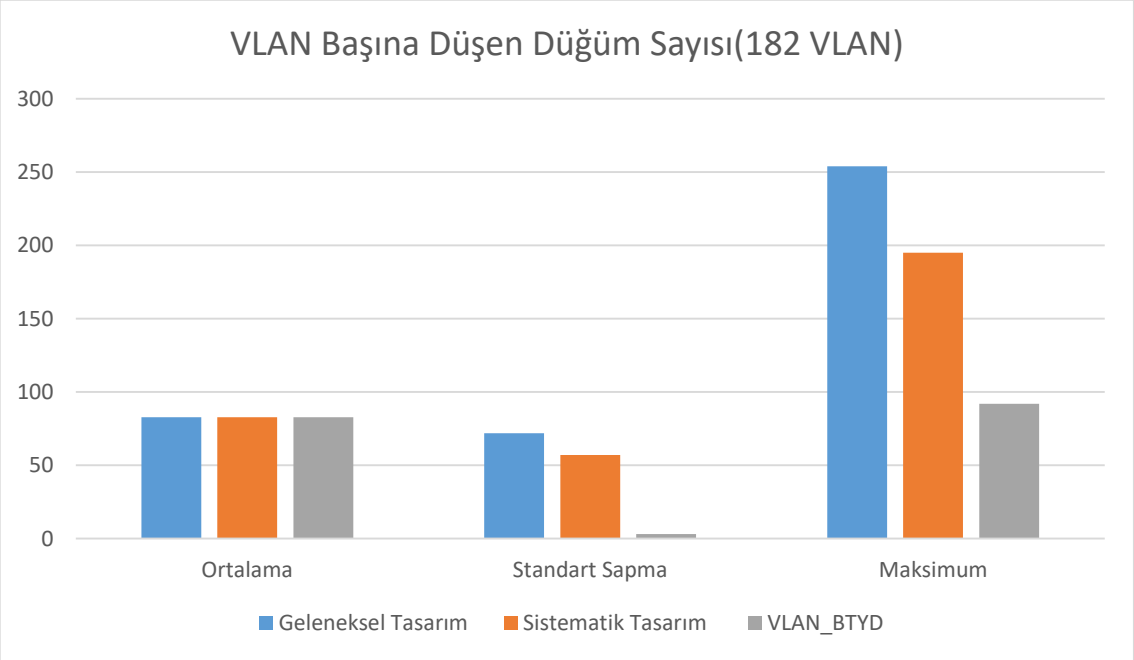
4.4.1. VLAN Başına Düğüm Sayısı Kriterine Göre Karşılaştırma

Kurumsal ağlar için sistematik tasarım yaklaşımının değerlendirilmesi için en önemli kriterlerden biri VLAN başına düşen düğüm sayısıdır [4]. Bu kısımda önerdiğimiz *VLAN_BTYD* algoritması kullanılarak sistematik ağ yaklaşımı ile Yu-Wei Eric Sung ve arkadaşlarının önerdiği yaklaşımdaki ve geleneksel tasarım için elde edilen VLAN başına düşen düğüm sayıları karşılaştırılmıştır.

VLAN_BTYD algoritmasına geleneksel ve sistematik yaklaşımın karşılaştırılması için kullanılan, her VLAN'da bulunması gereken ortalama düğüm sayısı kadar düğüm atanmıştır. *VLAN_BTYD* algoritmasının çalışması sonucunda en az 78 düğüm içeren VLAN ve en fazla 92 düğüm içeren VLAN'lar oluşmuş, Çizelge 4.12'de standart sapması ve maksimum değeri verilen düğüm sayıları elde edilmiştir.

Çizelge 4.12. VLAN başına düşen düğüm sayısı.

	VLAN Başına Düğüm Sayısı (182 VLAN)		
	Geleneksel Tasarım	Sistematik Tasarım	VLAN_BTYD
Ortalama	82,9	82,9	82,9
Standart sapma	71,9	57,1	3.1
Maksimum	254	195	92



Şekil 4.12. VLAN başına düşen düğüm grafiksel gösterimi

VLAN_BTYD algoritması için kullanılan düğümlerin ürettikleri trafik değerleri birbirlerine yakın olması nedeniyle maksimum düğüm sayısı ve ortalama düğüm sayısı birbirine yakın değerler çıkmaktadır. Bu nedenle *VLAN_BTYD* algoritması sonucu VLAN'lara dağılan düğüm sayılarının standart sapması da çok küçük bir değer olmaktadır. Karşılaştırılan diğer sistematik algoritmanın her düğümünün trafik değerleri birbirinden çok uzak olması nedeniyle standart sapması yüksek mevcut sistemlerin ise en yüksek değerde olduğu gözlemlenmiştir.

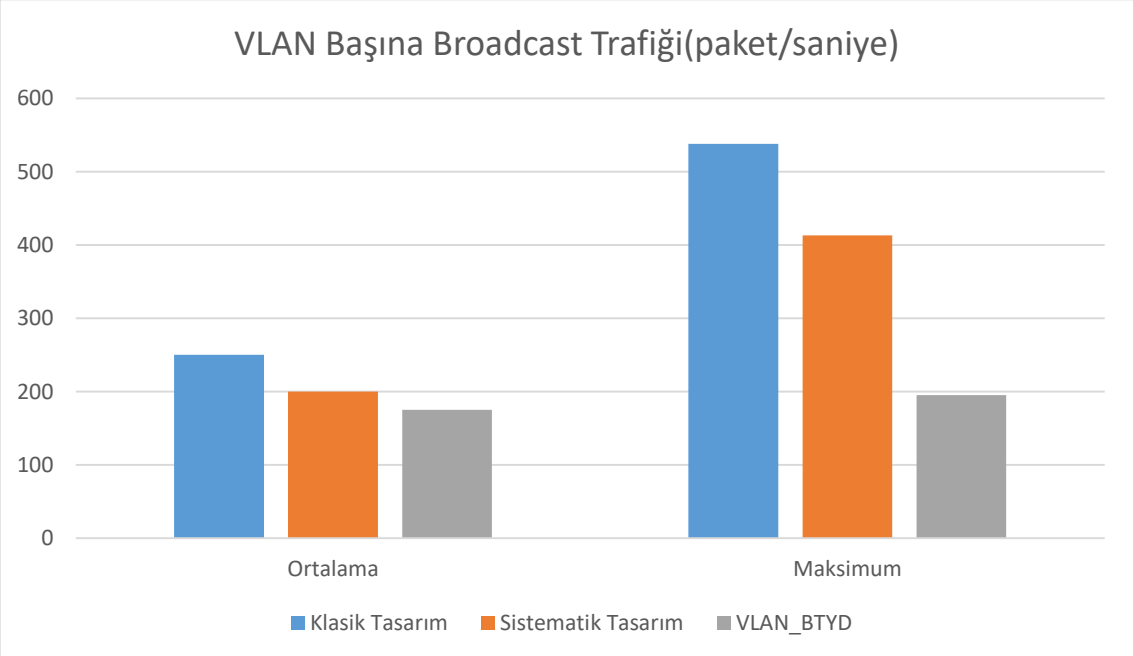
[4]'te Sistematik tasarımın klasik sisteme göre üstünlüğü olarak her bir VLAN'a dengeli düğüm dağıtımı konusunda iyileşme olduğu ifade edilmektedir. Önerdiğimiz yöntemde VLAN başına 3.1 standart sapma ile çok daha dengeli dağıtım gerçekleştirilmiştir.

4.4.2. Broadcast Trafik Kriterine Göre Karşılaştırma

Kurumsal ağlarda sistematik yaklaşımın değerlendirilmesi için kullanılan bir diğer kriter ağdaki broadcast trafiğidir. Ağda beklenen broadcast trafik değerleri klasik yöntemle tanımlanmış bir ağda ve sistematik olarak tasarlanmış bir ağ ile olan karşılaştırma sonuçları Çizelge 4.13'te verilmiştir. *VLAN_BTYD* algoritmasına, VLAN'lardaki ortalama paket sayısı [4]'te belirtildiği gibi, ağın en yoğun kullanımı esnasında düğümlerin ürettiği Çizelge 4.11'de verilen, düğüm başına üretilen maksimum broadcast trafiği parametresi kullanılarak, VLAN başına düşen düğüm sayısı ve anahtar başına düşen düğüm sayısı girdi olarak uygulanmış ve Çizelge 4.13'teki broadcast trafik değerleri elde edilmiştir.

Çizelge 4.13. Tahmini Broadcast trafiği değerleri

	VLAN Başına Broadcast Trafiği (paket/saniye)		
	Klasik Tasarım	Sistematik Tasarım	VLAN_BTYD
Ortalama	250	200	175
Maksimum	538	413	195



Şekil 4.13. VLAN başına Broadcast trafiği

Geleneksel ağda 24 saatlik zaman dilimlerinde yapılan ölçümlerde ortalama 0.004 paket/saniye/düğüm ve en fazla 2.12 paket/saniye/düğüm broadcast trafiği ölçülmüş

olduğundan sistematik tasarımda ve *VLAN_BTYD*'de aynı parametreler kullanılarak broadcast trafiği üretilmiştir. Yapılan hesaplamalar sonucunda Çizelge 4.13'te verilen VLAN başına ortalama ve maksimum broadcast trafiği değerleri elde edilmiştir.

Önerdiğimiz *VLAN_BTYD* yöntemi Çizelge 4.12'de verilen VLAN başına düşen düğüm sayısı açısından diğer yöntemlere göre daha dengeli dağıtım sağlamış olduğu için, ağlardaki broadcast trafiği değerleride diğer yöntemlere göre daha iyi sonuç vermiştir.

4.5. BENZER ÇALIŞMALARA KARŞI AVANTAJ VE DEZAVANTAJLARI

Bu çalışmanın 1. bölümü 4. kısmında değerlendirilen ve literatürdeki benzer çalışmalara göre, sunduğumuz yöntemin avantaj ve dezavantajları aşağıdaki kriterler doğrultusunda farklılıklar göstermektedir;

1. SNMP Protokolü ile uç cihazlardan veri alma.
2. SNMP Protokolü ile uç cihazlarda yapılandırma yapma.
3. SNMP Protokolü haricinde başka bir protokol ile 1 ve 2. maddeleri gerçekleştirme
4. Ağa ihtiyaç duyulduğunda dinamik olarak VLAN ekleme.
5. Güvenlik düzeylerine göre VLAN kullanımı.
6. Omurga anahtarda ACL ile çalışma.
7. Omurga anahtarda VLAN'ların tanımlanması zorunluluğu.
8. Düğümlerin ürettikleri trafiklere göre VLAN üyeliklerinin değişmesi.
9. Merkezi bir sunucuda ağ bilgilerini değerlendirme.
10. Çalışmanın gerçek ortamda test edilmesi.
11. Marka bağımsız çalışma.
12. OpenFlow Protokolü Kullanımı.

Bu kriterlere göre literatürde yer alan benzer çalışmaların karşılaştırılması maksadıyla Çizelge 4.14'te detaylı olarak verilmiştir.

Çizelge 4.14. Çalışmanın kriterlere göre diğer çalışmalar ile karşılaştırılması.

Benzer Çalışmalar	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
VLAN_BTYD	✓	✓	✕	✓	✓	✕	✓	✓	✓	✓	✓	✕
MAC Based Dynamic VLAN Tagging with OpenFlow for WLAN Access Networks	✕	✕	✓	✕	✓	✕	✓	✕	✓	✓	✓	✓
A Method of Dynamic Interconnection of VLANs for Large Scale VLAN Environment	✕	✕	✓	✕	✓	✕	✓	✕	✓	✓	✓	✕
Kurumsal Kampüs Ağlarında Otomatik Sanal Yerel Alan Ağ Tasarımları ve Servis Kalitesi Analizleri	✕	✕	✓	✕	✓	✓	✓	✕	✓	✓	✓	✕
Application Of Dynamic Port VLAN Membership with Auxiliary VLAN In Campus Area Network	✕	✕	✓	✕	✓	✕	✓	✓	✓	✓	✕	✕
Towards Systematic Design of Enterprise Networks	✕	✕	✓	✓	✓	✕	✓	✓	✓	✕	✓	✕
Finding Efficient VLAN Topology For BetterBroadcast Containment	✕	✕	✓	✓	✕	✕	✓	✓	✓	✕	✓	✕
CSS-VM : A Centralized and Semi-automatic System for VLAN Management	✓	✕	✓	✕	✓	✕	✓	✕	✓	✓	✓	✕
Effective VTP Model for Enterprise VLAN Security	✕	✕	✓	✕	✓	✓	✓	✕	✓	✕	✕	✕

5. SONUÇLAR VE ÖNERİLER

5.1. SONUÇLAR

Bu çalışmada LAN'da bulunan VLAN'lara üye olan düğümlerin toplam trafiklerini değerlendiren, her bir VLAN'ın toplam trafiklerini birbirlerine yakın veya eşit yapmaya yönelik yeni bir algoritma geliştirilmiştir. *VLAN_BTYD* adını verdiğimiz bu algoritma aynı zamanda ihtiyaç duyulduğunda ağda yeni bir VLAN oluşturarak bu VLAN'a yeni düğümler atamamıza da olanak sağlamaktadır.

Aşağıda, yapılan çalışmalar, tezin sunumuna uygun olarak kısaca hatırlatılmış ve elde edilen bulgular sunulmuştur.

1. LAN'lar, yönetilebilirlik, esneklik ve kolay gözlemlenebilmeleri açısından VLAN'lara bölünebilirler. VLAN'lar farklı türlere sahiptirler. Bu çalışmada bu türlerden dinamik VLAN türüne değinilmiştir. Bunun sebebi bu çalışmada LAN'da bulunan VLAN sayısının, sahip olduğu toplam trafik değerine bağlı olarak arttırılabilmesi ve aynı zamanda kendisine üye olan düğümlerin değişebilmesidir. Bölüm 1'de VLAN'lar hakkında detaylı bilgi sunulmuştur.
2. Literatürde yer alan ve çalışmamızla benzerlik gösteren çalışmalar araştırılmış, çalışmamıza göre avantajları ve dezavantajları Bölüm 1'de detaylı olarak verilmiştir. Çalışmanın en önemli avantajlarından biri SNMP V3 protokolü desteklemesi şartı ile mevcut cihazların bulunduğu herhangi bir VLAN barındıran ağda uygulanabilir olmasıdır. Böylelikle maliyet açısından herhangi bir yük getirmeyeceği gibi ağın broadcast trafiğinden doğan gecikmelerinin önüne geçilmesi sağlanmıştır.
3. LAN'da bulunan anahtarların yönetilebilmeleri birkaç farklı yolla yapılabilir. Ancak şifreli haberleşme ve kimlik doğrulama mekanizmalarına sahip olması ve marka bağımsız çalışabilmesi üstünlüğünden dolayı bu çalışmada SNMP V3 protokolü seçilmiştir. Geliştirilen algoritmada SNMP V3 protokolünün sağladığı avantajlar kullanılmıştır.
4. Algoritmanın matematiksel modeli çıkartılmış ve akış diyagramları Bölüm 3'te

detaylı bir şekilde sunulmuştur.

5. Literatürde bu tez çalışmasına yaklaşım ve metodoloji bakımından benzer çalışmalar, belirli kriterler seçilerek karşılaştırmalı olarak Bölüm 4'te bir tablo halinde verilmiştir.
6. Önerdiğimiz yöntemin performans değerlendirmesini yapabilmek için deneysel ortam oluşturulmuştur.
    a. Bu algoritmanın uygulanması için Visual Studio geliştirme ortamında C# programlama dili ile masaüstü bir uygulama geliştirilmiştir.
    b. Düğümlerin ve uç cihazların bilgilerini tutmak için MS-SQL veritabanı kullanılmıştır.
    c. Ortamda farklı VLAN'larda kullanılmak üzere üzerinde IP aralıkları tanımlanmış bir DHCP sunucusu kurulmuştur.
    d. Her bir anahtar üzerinde varsayılan VLAN tanımlanmıştır.
    e. Ağa takılan her anahtar için bütün portlar varsayılan VLAN'a üye yapılmıştır.
7. Performans ve değerlendirmeler için gerekli koşullar ve kabuller olmak zorundadır. Bunlar geliştirilen algoritmanın uygulanması için geliştirilen yazılımın ve ağ ortamının ihtiyaçlarıdır. Algoritmanın belirlenen hedeflere ulaştığını göstermek maksadıyla, Bölüm 4'te verilen kabullerin sağlandığı gerçek bir ağ ortamında testler yapılmıştır. Bu testler;
    a. Ağa yeni bir düğüm bağlandığında nasıl davrandığını,
    b. Ağda önceden bağlı bir düğümün ayrılıp geri geldiğinde nasıl bir erişime tabi olacağı,
    c. Algoritma çalışma döngüsü sonucu trafik değerlerine göre düğümlerin yeni üyeliklerinin nasıl olacağı,
    d. Ağda düğüm ve trafik artışına göre algoritmanın tepkisinin ne olacağı,
    e. Güvenlik düzeyine sahip bir düğümün ağa değişik konumlardan bağlanması ve ayrılması sonucu algoritmanın nasıl bir sonuç ortaya koyacağı,
    f. Belirlenen eşik değerine göre yeni bir VLAN oluşturulması ve bu VLAN'a

trafik değerlerinin birbirlerine yakın VLAN'lar oluşturulması hedefi doğrultusunda yeni düğümler atanması işlemi gerçekleştirilmesi,

gibi farklı senaryolar ile gerçekleştirilmiştir.

8. Senaryolar algoritmanın başlangıçta ortaya konan hedefler doğrultusunda çalıştığını göstermiştir. Bu bağlamda test sonuçlarına göre;
    a. Ağa yeni dahil olan düğüm trafik değeri en az VLAN'a üye olmuştur.
    b. Güvenlik düzeyi farklı VLAN'a üye düğümler ağın her noktasından kendi hakları çerçevesinde ağa dahil olmuşlardır.
    c. Düğüm sayısı ve trafik miktarı artsa bile algoritma çalışma döngüsü sonucu VLAN'ların trafik değerlerinin birbirlerine çok yakın gerçekleştiği görülmüştür.
    d. Belirlenen eşik değerine göre ağda yeni VLAN oluşumu gerçekleşmiş ve düğümler bu VLAN'a amaç doğrultusunda üye olmuştur.
9. Performans değerlendirmesi için *VLAN_BTYD* algoritmasına literatürde yer alan [4] numaralı çalışma ile aynı ortam değişkenleri uygulanmıştır.
    a. Değerlendirme kriterlerinden biri olan VLAN başına düşen düğüm sayılarının, karşılaştırılan diğer iki yönteme göre daha eşit dağılımlı sonuçlar verdiği, dağılımın standart sapmasının düşük olduğu ve maksimum düğüm sayısı ile ortalama düğüm sayılarının birbirine yakın değerler olduğu görülmüştür. Buda algoritmanın hedef doğrultusunda doğru ve daha başarılı sonuçlar ortaya koyduğu anlamına gelmektedir.
    b. Diğer değerlendirme kriteri olan VLAN başına düşen broadcast trafiği değerlendirmesidir. Bu kriter açısından *VLAN_BTYD* algoritması, VLAN'lar arası broadcast trafiğinin diğer iki yönteme göre dağılımın daha dengeli yaptığını göstermektedir. *VLAN_BTYD* algoritması VLAN'ların eşit ya da birbirine yakın trafik değerlerine göre şekillenmesini hedeflemektedir. Bu karşılaştırma, bu kritere göre algoritmanın hedefine ulaştığını göstermiştir.

Sonuç olarak önerilen yöntem Ethernet anahtarların markadan bağımsız olarak SNMP desteğine sahip anahtarlardan oluşan tüm ağlarda uygulanabilir olması açısından literatürde yer alan yöntemlere göre üstünlüğe sahiptir ve bilime bu bağlamda katkı sağlanmıştır.

5.2. ÖNERİLER

Bu tez çalışmasında, algoritmanın her döngü çerçevesinde bir önceki döngü ile arasında geçen süredeki toplam trafikler baz alınmıştır. Bu nedenle ilerde yapılacak çalışmada istatiksel olarak ağdaki düğüm bazlı trafikler değerlendirilerek karar verme aşaması gerçekleştirilebilir.

Bu çalışmada Spanning Tree Protocol kullanılmamıştır. Spanning Tree Protocol kullanılması durumunda sonuçlar için algoritma güncellenebilir.

Bu çalışmada ağın dinlenmesi, anahtarlardan bilgi toplanıp değerlendirilmesi çerçevesinde çalışılmıştır. Ancak yeni bir yaklaşım olan SDN ile anahtar cihazların dinlenmesi gibi ek yükler olmaksızın veriler elde edilebileceğinden, çalışmadaki bu yaklaşım SDN kullanılarak daha verimli bir şekilde gerçekleştirilebilir. Ancak bunun yapılabilmesi için ağda kullanılacak olan anahtarların SDN'in kullandığı OpenFlow protokolünü desteklemesi gerekmektedir.

Ağ belirli aralıklar ile dinlendiği için olağan dışı ağ trafikleri oluşturan düğümler tespit edilebilir. Ağ yöneticisi bu düğümler hakkında bilgilendirilebilir veya otomatik olarak ağa erişmesi engellenebilir.

VTP protokolü kullanıldığında VLAN atlatma gibi ataklar için test yapılmamıştır. Bu saldırı tekniğine karşı algoritma revize edilebilir.

Algoritma çağırılma zamanları sonrası, VLAN'ı değişen her bir düğümün ağ bağlantısı koparılıp tekrar aktif edilmektedir. Bu esnadaki kesintilerin önüne geçebilmek için yeni bir çalışma yapılabilir.

5.3. ÇALIŞMANIN GETİRDİĞİ KATKILAR

Bu çalışmanın bilime ve teknolojiye getirdiği ana katkılar aşağıda maddeler halinde verilmiştir.

1. Kurumsal ağlar için VLAN'lar arasında dengeli trafik dağılımı olacak şekilde dinamik VLAN üyeliğine imkan sağlayan yeni bir yöntem geliştirilmiştir.
2. Kurumların ve firmaların mevcut ağlarında bulunan Ethernet anahtarları üzerinde çalışabilen bir trafik yük dengelemesi algoritması geliştirilerek maliyet açısından avantaj sağlanmıştır.
3. SNMP protokolünün 3. versiyonu kullanarak ağ cihazları arasında ve ağ cihazları ile kontrolcü arasında aktarılan kontrol trafiğinin güvenliği sağlanmıştır.
4. Yenilikçi ağ yaklaşımı olan yazılım tabanlı ağlar (SDN) ile yeni ağ cihazları kullanılarak kurumsal ağlara eklenebilecek yeni servislerin ve özelliklerin geleneksel ağ cihazları kullanılan ağlarda da çalıştırılabileceği gösterilmiştir.

6. KAYNAKLAR

[1] X. Sun, Y. Sung, S. D. Krothapalli and S. G. Rao, "A systematic approach for evolving VLAN designs," in *IEEE International Conference on Computer Communications*, San Diego, CA, USA, 2010, pp. 1-9.

[2] D. Maltz, G. Xie, and J. Zhan, "Routing design in operational networks: A look from the inside," in *SIGCOMM '04 Proceedings Of The 2004 Conference On Applications, Technologies, Architectures, And Protocols For Computer Communications*, Portland, Oregon, USA, 2004, pp. 27-40.

[3] F. Le, G. G. Xie, D. Pei, J. Wang, and H. Zhang, "Shedding light on the glue logic of the internet routing architecture," in *SIGCOMM '08 Proceedings Of The ACM SIGCOMM 2008 Conference On Data Communication*, Seattle, WA, USA, 2008, pp. 39–50.

[4] Y. E. Sung, X. Sun, S. G. Rao, G. G. Xie, and D. A. Maltz, "Towards systematic design of enterprise networks," *IEEE/ACM Transactions on Networking*, vol. 19, no. 3, pp. 695–708, 2011.

[5] P. Garimella, P. Garimella, Y. Sung, N. Zhang, and S. Rao, "Characterizing VLAN usage in an operational network characterizing VLAN usage in an operational network," in *INM '07 Proceedings Of The 2007 SIGCOMM Workshop On Internet Network Management*, Kyoto, Japan, 2007, pp. 305–306.

[6] G.G. Xie , Jibin Zhan , D.A. Maltz , Hui Zhang , A. Greenberg , G. Hjalmtysson and J. Rexford, "On static reachability analysis of IP networks," in *IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies*, Miami, FL, USA, 2005, pp. 2170–2183.

[7] Z. Kerravala, "Configuration management delivery business resiliency," The Yankee Group, Boston, 2002.

[8] S. Narain and T. Technologies, "Network configuration management via model finding," in *LISA '05 Proceedings of the 19th Conference On Large Installation System Administration Conference*, San Diego, CA,USA, 2005, p. 15.

[9] Z. S. Guo and Y. Zhuang, "Improving network performance by traffic reduction," in *Proceedings of ICICS, 1997 International Conference on Information, Communications and Signal Processing. Theme: Trends in Information Systems Engineering and Wireless Multimedia Communication*s, Singapore, Singapore 1997, pp. 1226–1230.

[10] V. Rajaravivarma, "Virtual local area network technology and applications," in *The Twenty-Ninth Southeastern Symposium on System Theory*, Cookeville, TN, USA, 1997, pp. 49–52.

[11] A. Aktaş, "VLAN teknolojisi ile kampüs ağında aşırı istenmeyen paket trafiğin önlenmesi," Yüksek Lisans tezi, Elektrik Elektronik Mühendisliği EABD, Gaziantep Üniversitesi, Gaziantep, Türkiye, 2016.

[12] K. İlhan, "Bilgisayar ağı güvenlik sisteminin çok ölçütlü seçimi ve AHP uygulaması," Yüksek Lisans tezi, Endüstri Mühendisliği EABD, Dumlupınar Üniversitesi, Dumlupınar, Türkiye, 2009.

[13] T. Cambazoğlu, "Internet ve Güvenlik", Savunma Sanayii Müsteşarlığı, Türkiye,

Rap. 78, 2003.

[14] Extreme Networks. (2005.October.05). *Approach to Information Security: Protection User Data Flow*. [Online]. Avaliable: http://www.dienekis.gr/resource/papers/extreme011.pdf

[15] M. Çetin, "Kurumsal kampüs ağlarında otomatik sanal yerel alan ağ tasarımları ve servis kalitesi analizleri," Yüksek Lisans tezi, Elektrik Elektronik Mühendisliği EABD, Pamukkale Üniversitesi, Pamukkale, Türkiye, 2006.

[16] D. P. Gilliam, T. L. Wolfe, J. S. Sherif, and M. Bishop, "Software security checklist for the software life cycle," in *Wet Ice 2003. Proceedings. Twelfth Ieee International Workshops On Enabling Technologies: Infrastructure For Collaborative Enterprises*, Linz, Austria, 2003, pp. 243–248.

[17] G. Mcgraw, "Software security," *IEEE Security & Privacy*, vol. 2, no. 2, pp. 80–83, 2004.

[18] M. Koerner and O. Kao, "MAC based dynamic VLAN tagging with OpenFlow for WLAN access networks," *Procedia Computer Science*, vol. 94, pp. 497–501, 2016

[19] K. Kawano, T. Okamoto, K. Okayama, N. Yamai and T. Miyashita, "A method of dynamic ınterconnection of VLANs for large scale vlan environment," in *6th Asia-Pacific Symposium on Information and Telecommunication Technologies*, Yangon, Myanmar 2005, pp. 427–432.

[20] N. Jiang, L. Shan, and J. Zhao, "Application of dynamic port VLAN membership with auxiliary VLAN in campus area network," in *9th International Conference on Hybrid Intelligent Systems*, Shenyang, LiaoNing, China, 2009, pp. 279–282.

[21] VMware, (2012.01.March). *VMware vSphere Distributed Switch Best Practices* [Online]. Available: https://www.vmware.com/content/dam/digitalmarketing/ vmware/en /pdf/ techpaper/ vsphere-distributed-switch-best-practices-white-paper.pdf .

[22] A. Hameed and A. N. Mian, "Finding efficient VLAN topology for better broadcast containment," in *2012 Third International Conference on The Network of the Future*, Gammarth, Tunisia, 2012, pp. 1–6.

[23] F. Li, J. Yang, C. An, J. Wu, S. Wang, and N. Jiang, "CSS-VM : A Centralized and Semi-automatic system for VLAN management," in *2013 IFIP/IEEE International Symposium on Integrated Network Management*, Ghent, Belgium, 2013, pp. 623–629.

[24] R. O. Verma and S. S. Shriramwar, "Effective VTP model for enterprise VLAN security," in *2013 International Conference on Communication Systems and Network Technologies Effective*, Gwalior, India, 2013, pp. 426–430.

[25] A. Pérez-Méndez, F. Pereñíguez-García, R. Marín-López, G. López-Millán, and J. Howlett, "Identity federations beyond the web: A survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, pp. 2125–2141, 2014.

[26] M. Yu and J. Rexford, "Topıcs ın network and servıce management a survey of virtual lan usage in campus networks," *IEEE Communications Magazine*, vol.49, pp. 98–103, 2011.

[27] Y. Yamasaki, "Flexible access management system for campus VLAN based on OpenFlow," in *IEEE/IPSJ International Symposium on Applications and the*

Internet, Munich, Bavaria, Germany, 2011, pp. 347–351.

[28] Y. Nagatomo, H. Nishino, and T. Kagawa, "An AR-Based VLAN visualizer," in *IEEE International Conference on Consumer Electronics*, Taipei, Taiwan, 2014, pp. 117–118.

[29] A. Tekerek, C. Gemci, ve Ö. F. Bay, "Web tabanli saldiri önlemsistemi tasarimi gerçekleştirilmesi: yeni bihibrit model," *Gazi Üniversitesi Mühendislik-Mimarlık Fakültesi Dergisi*., c. 31, s. 3, ss. 645–653, 2016.

[30] E. Irmak ve A. Calpbinici, "e-laboratuvarla için yenibir tasarim: eş zamanerişilebilen deneysel uygulama platformu," *Gazi Üniversitesi Mühendislik-Mimarlık Fakültesi Derg*isi, c. 32, s. 2, ss. 363–375, 2017.

[31] Z. Li, Z. Hu, G. Zhang, and Y. Ma, "Ethernet topology discovery for virtual local area networks with incomplete information," in *4th IEEE International Conference on Network Infrastructure and Digital Content*, Beijing, China, 2014, pp. 252–256.

[32] S. Pandey, M. Choi, S. Lee, and J. Hong, "IP network topology discovery using SNMP." in *International Conferance on Information Networking*, Chiang Mai, 2009, pp. 1-5.

[33] O. Ergün, (2018.April.26). *What is Vlan load balancıng?*. [Online]. Available: https://orhanergun.net/2016/05/vlan-load-balancing/.

[34] M. Balta and İ. Özçelik, "The discovery of enterprise network topology created in a virtual environment with SNMPv3," *The Association Of Science, Education And Technology*, vol. 2, no. 2, pp. 64–70, 2012.

[35] M. Balta, "Sanal ortam üzerinde oluşturulan örnek bir kurumsal ağ topolojisinin SNMPv3 ile topoloji keşfi uygulaması," Yüksek Lisans tezi, Sakarya Üniversitesi, Sakarya, Türkiye, 2012.

[36] J. F. Kurose and K. W. Ross, *Computer Networking A Top-Down Approach Featuring The İnternet*, 6th ed., Boston, USA: Addison-Wessley, 2012 , ch. 9, pp-775.

[37] M. Subramanian, *Network management, principles and practice*, , Delhi, Indian: Addison-Wessley, 2010, ch. 3, pp 170-307.

[38] A. Affandi, D. Riyanto, I. Pratomo, and G. Kusrahardjo, "Design and implementation fast response system monitoring server using simple network management protocol (SNMP)," in *International Seminar on Intelligent Technology and Its Applications (ISITIA)*, Surabaya, Indonesia, 2015, pp. 385–390.

[39] Charles M. Kozierok, (2018.February.08), "*SNMP terminology summary*," [Online]. Available: http://www.tcpipguide.com /free/ t_TCPIPSNMP OperationalModel Componentsand Terminology-3.htm.

[40] *A Simple Network Management Protocol (SNMP)*, rfc1157, 1990.

[41] J. Li, "WEB-based Network Monitoring Using SNMP, CG1 and CORBA," M.S. thesis, Manitoba University, Manitoba, Kanada, 1999.

[42] A. Iqbal, C. Pattinson, and A. L. Kor, "Managing energy efficiency in the cloud computing environment using SNMPv3: a quantitative analysis of processing and power usage," in *IEEE 14th International Conference on Dependable, Autonomic and Secure Computing, DASC 2016, 2016 IEEE 14th International Conference on*

Pervasive Intelligence and Computing, PICom 2016, 2016 IEEE 2nd International Conference on Big Data, Auckland, New Zealand, 2016, pp. 239–244.

[43] *SNMP V3 Applications*, rfc2273, 1998.

[44] B. Rane Douglas. (2005.January.23), *SNMP: Simple? Network Management Proto*col [Online]. Available: http://www.rane.com/note161.html.

[45] B. Rane Douglas. (2005.January.23). *SNMP Simple Network Management Protocol* [Online]. Available: http://www.rane.com/ pdf/ranenotes /SNMP_Simple_ Network_Management_Protocol.pdf.

[46] Addison Wesley Longman (2001.January.01). *The Internet Network-Management Framework.* [Online]. Available: http://netlab.ulusofona.pt/rc/book/8-management/8_03/index.htm.

[47] H3C. (2018.February.01). *SNMP Technology White Paper*. [Online]. Available: http://www.h3c.com.hk/products_technology/products/switches/data_centre_switches/h3c_s5800s5820_series_switches/white_paper/200912/656271_57_0.htm.

[48] B. J. Leon, "A formal approach to model SNMP network management systems," in *Fourth International Conference on Computer Communications and Networks - IC3N'95*, Las Vegas, NV, USA, 1995, pp. 284–287.

[49] A. M. Koth, A. El-Sherbini and T. Kamel, "A new interoperable management model for IP and OSI architectures," in *IEEE. AFRICON '96*, Stellenbosch, South Africa, vol.2, pp. 944-949, 1996.

[50] LoriotPro. (2018.January.24). *Administrator Book SNMP Objects Loriot Pro v3*. [Online]. Available: http://www.loriotpro.com /Products/On-line_ Documentation V3 / LoriotProV3Doc /C3-Introduction_ to_ Network_ Supervision / C3-D4_SNMP_Object.htm.

[51] Free Software Foundation. (2007. March.29). *SnmpSharpNet*. [Online]. Available: https://www.snmpsharpnet .com.

[52] Douglas E. Comer, *Bilgisayar Ağları Ve İnternet*, Ankara, Türkiye:Nobel Akademik Yayıncılık, 2016, böl.8, ss-475.

[53] Ostinato, *Bilgisayar Programı*, Ağ trafik üretici ve analiz edici program, 2018.

ÖZGEÇMİŞ

KİŞİSEL BİLGİLER

Adı Soyadı : Serdar KIRIŞOĞLU

Doğum Tarihi ve Yeri : 10.04.1982 KASTAMONU

Yabancı Dili : İngilizce

E-posta :serdarkirisoglu@duzce.edu.tr

ÖĞRENİM DURUMU

Derece	Alan	Okul/Üniversite	Mezuniyet Yılı
Doktora	Elektrik Elektronik ve Bilgisayar A.B.D.	Düzce Üniversitesi	2018
Y. Lisans	Elektrik Eğitimi A.B.D.	Abant İzzet Baysal Üniversitesi	2009
Lisans	Elektrik Elektronik Müh.	Kahramanmaraş Sütçü İmam Üniversitesi	2005
Lise		Mustafa Kaya Anadolu Lisesi	2000

YAYINLAR

1. KIRIŞOĞLU S., KARA R., ÖZÇELİK İ., "Sanal Yerel Alan Ağlarında Ağ Trafiği Dengeleme İçin SNMP Tabanlı Yeni Bir Algoritma" Gazi Üniversitesi Mühendislik-Mimarlık Fakültesi Dergisi,2018,2018
2. KIRIŞOĞLU S., DÖŞOĞLU M.K., ÖZTÜRK A., "Matematiksel İşlemlerin Matlab Gui'de Analizi", 5. Uluslararası İleri Teknolojiler Sempozyumu (IATS'09)Karabük, Türkiye,2009,136-138
3. KIRIŞOĞLU S., ERCAN İ., KARA R., "LSB Metodunu Kullanarak Sayısal

Görüntüye Veri Gizlemek İçin FPGA Modülü Geliştirilmesi", 4. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, Ankara, Türkiye, 2010, 206-211

4. KIRIŞOĞLU S., ERCAN İ., ŞAHİN İ., "Sayısal Görüntüye Veri Gömmek Ve Ayrıştırmak İçin FPGA Tabanlı Donanım Modülü Tasarımı", Gömülü Sistemler ve Uygulamaları Sempozyumu, İstanbul, Türkiye, 2008, 27